

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 1999年 8月27日

出願番号
Application Number: 平成11年特許願第241747号

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号
the country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 1 9 9 9 - 2 4 1 7 4 7

願人
Applicant(s):

富士通株式会社
株式会社日立製作所
コロムビアミュージックエンタテインメント株式会社
三洋電機株式会社

2006年 8月22日

特許庁長官
Commissioner,
Japan Patent Office

中 嶋 誠



【書類名】 特許願

【整理番号】 1990901

【提出日】 平成11年 8月27日

【あて先】 特許庁長官殿

【国際特許分類】 H04M 11/08

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 畑中 正行

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 蒲田 順

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 畠山 卓久

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 長谷部 高行

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 小谷 誠剛

【発明者】

【住所又は居所】 東京都小平市上水本町 5 丁目 2 0 番 1 号 株式会社日立製作所 半導体グループ内

【氏名】 木下 泰三

【発明者】

【住所又は居所】 東京都港区赤坂四丁目 1 4 番 1 4 号 日本コロムビア株式会社内

【氏名】 穴澤 健明

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 日置 敏昭

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 金森 美和

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 堀 吉宏

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

【氏名又は名称】 富士通株式会社

【特許出願人】

【識別番号】 000005108

【住所又は居所】 東京都千代田区神田駿河台 4 丁目 6 番地

【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 000004167

【住所又は居所】 東京都港区赤坂四丁目 1 4 番 1 4 号

【氏名又は名称】 日本コロムビア株式会社

【特許出願人】

【識別番号】 000001889
【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号
【氏名又は名称】 三洋電機株式会社

【代理人】

【識別番号】 100064746
【弁理士】
【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132
【弁理士】
【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409
【弁理士】
【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781
【弁理士】
【氏名又は名称】 堀井 豊

【手数料の表示】

【予納台帳番号】 008693
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ配信システム

【特許請求の範囲】

【請求項 1】 コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第 1 のインターフェース部と

前記暗号化コンテンツデータの通信ごとに更新される第 1 の共通鍵を生成する第 1 のセッションキー発生部と、

前記ユーザの端末に対応して予め定められた第 1 の公開暗号化鍵により前記第 1 の共通鍵を暗号化して前記第 1 のインターフェース部に与えるためのセッションキー暗号化部と、

前記第 1 の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、

前記暗号化コンテンツデータを復号するためのコンテンツキーを、前記セッションキー復号部により復号されたデータを鍵データとして暗号化するための第 1 のライセンスデータ暗号処理部と、

前記第 1 のライセンスデータ暗号処理部の出力を第 2 の共通鍵でさらに暗号化して前記第 1 のインターフェース部に与え配信するための第 2 のライセンスデータ暗号処理部とを備え、

各前記端末は、

外部との間でデータを授受するための第 2 のインターフェース部と、

前記暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、

前記配信データ解読部は、

前記第 1 の公開暗号化鍵によって暗号化されたデータを復号化するための第 1 の秘密復号鍵を保持する第 1 の鍵保持部と、

前記第 1 の公開暗号化鍵によって暗号化された前記第 1 の共通鍵を受けて、復号処理するための第 1 の復号処理部と、

第 2 の公開暗号化鍵を保持するための第 2 の鍵保持部と、

前記第 2 の公開暗号化鍵を、前記第 1 の共通鍵に基づいて暗号化し、前記第 2 のインターフェース部に出力するための第 1 の暗号化処理部と、

前記第 2 のライセンスデータ暗号処理部からの暗号化されたコンテンツキーを受け、前記第 2 の共通鍵に基づいて復号化するための第 2 の復号処理部と、

前記第 2 の復号処理部の出力を受けて、格納するための第 1 の記憶部と、

前記第 2 の公開暗号化鍵によって暗号化されたデータを復号化するための第 2 の秘密復号鍵を保持する第 3 の鍵保持部と、

前記第 1 の記憶部に格納されたデータに基づいて、前記第 2 の秘密復号鍵により前記コンテンツキーを復号するための第 3 の復号処理部とを備える、データ配信システム。

【請求項 2】 前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第 1 の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた鍵であり、

前記第 2 の秘密復号鍵は、前記メモリカードごとに異なる、請求項 1 記載のデータ配信システム。

【請求項 3】 前記第 2 および第 3 の復号処理部は、前記コンテンツデータ供給装置において前記第 2 の公開暗号化鍵で暗号化され、さらに前記第 2 の共通鍵で暗号化されて、前記コンテンツキーとともに配信されるライセンス情報データを前記第 2 のインターフェース部を介して受け、前記第 2 の共通鍵および前記第 2 の秘密復号鍵に基づいて復号し、

前記配信データ解読部は、

復号された前記ライセンス情報データを格納する第 2 の記憶部をさらに備える、請求項 2 記載のデータ配信システム。

【請求項 4】 前記第 1 の共通鍵と前記第 2 の共通鍵とは、前記暗号化コンテンツデータの通信の際に、前記第 1 のセッションキー発生部により生成された同一の鍵データである、請求項 3 記載のデータ配信システム。

【請求項 5】 前記第 1 の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格

納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第 1 の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第 3 の復号処理部からの前記コンテンツキーを受けて、第 3 の共通鍵に基づいて暗号化して出力し、

前記第 1 の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第 3 の共通鍵を生成する第 2 のセッションキー発生部と、

前記配信データ解読部からの前記第 3 の共通鍵により暗号化された前記コンテンツキーを受けて復号して抽出し、前記第 1 の記憶部から出力された前記暗号化コンテンツデータを前記コンテンツキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項 4 記載のデータ配信システム。

【請求項 6】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第 3 の公開暗号化鍵で暗号化処理を行なうための第 2 の暗号化処理部とをさらに含み、

前記第 2 の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第 3 の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第 3 の公開暗号化鍵を復号して抽出し、

前記第 2 の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記コンテンツキーおよび前記ライセンス情報データを前記第 3 の公開暗号化鍵で暗号化し、

前記第 1 の暗号化処理部は、前記第 2 の暗号化処理部の出力を受けて、前記第 3 の共通鍵に基づいて暗号化して前記第 2 のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第 2 の記憶部に格納されている前記ライセンス情報データを消去し、

前記第 1 の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 5 記載のデータ配信システム。

【請求項 7】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第 1 の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 5 記載のデータ配信システム。

【請求項 8】 前記配信データ解読部は、

前記第 2 の共通鍵を生成するための第 3 のセッションキー発生部と、

前記第 3 のセッションキー発生部の出力を暗号化して前記第 2 のインターフェース部に与えることが可能な第 3 の暗号化処理部とをさらに含む、請求項 3 記載のデータ配信システム。

【請求項 9】 前記第 1 の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第 3 の暗号処理部は、第 4 の公開暗号化鍵により前記第 3 のセッションキー発生部の出力を暗号化して前記第 2 のインターフェース部に与え、

前記第 1 の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータ

の再生動作が指示されるのに応じて、前記第 3 の復号処理部からの前記コンテンツキーを受けて、第 3 の共通鍵に基づいて暗号化して出力し、

前記第 1 の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第 3 の共通鍵を生成する第 2 のセッションキー発生部と、

前記第 4 の公開暗号化鍵を前記配信データ解読部に与える公開鍵保持部と、

前記第 4 の公開暗号化鍵で暗号化された前記第 2 の共通鍵を復号可能な公開鍵復号部と、

前記配信データ解読部からの前記第 3 の共通鍵により暗号化された前記コンテンツキーを受けて復号して抽出し、前記第 1 の記憶部から出力された前記暗号化コンテンツデータを前記コンテンツキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項 8 記載のデータ配信システム。

【請求項 10】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第 3 の公開暗号化鍵で暗号化処理を行なうための第 2 の暗号化処理部とをさらに含み、

前記第 2 の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第 3 の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第 3 の公開暗号化鍵を復号して抽出し、

前記第 2 の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記コンテンツキーおよび前記ライセンス情報データを前記第 3 の公開暗号化鍵で暗号化し、

前記第 1 の暗号化処理部は、前記第 2 の暗号化処理部の出力を受けて、前記第 3 の共通鍵に基づいて暗号化して前記第 2 のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第 2 の記憶

部に格納されている前記ライセンス情報データを消去し、

前記第 1 の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 9 記載のデータ配信システム。

【請求項 1 1】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第 1 の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 9 記載のデータ配信システム。

【請求項 1 2】 前記第 1 のインターフェース部と前記第 2 のインターフェース部とは、携帯電話網により接続され、

前記コンテンツデータ供給装置は、

前記第 1 の公開暗号鍵に基づいて、前記ユーザの認証を行なう、請求項 1 記載のデータ配信システム。

【請求項 1 3】 前記第 1 のインターフェース部は、

前記端末と直接接続可能なコネクタ部を含む、請求項 1 記載のデータ配信システム。

【請求項 1 4】 前記第 1 のインターフェース部は、

前記メモリーカードと直接接続可能な接続部を含む、請求項 2 記載のデータ配信システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、携帯電話等の端末に対して情報を配送するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムに関するものである。

【0 0 0 2】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0 0 0 3】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

【0 0 0 4】

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0 0 0 5】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物情報の配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0 0 0 6】

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽情報のコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行う個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

【0 0 0 7】

しかも、CDからMDへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、1つのM

Dからさらに他のMDに音楽情報をデジタル情報としてコピーすることは、著作権者保護のために機器の構成上できないようになっている。

【0 0 0 8】

すなわち、現状においては、デジタル記録媒体であるCDからMDへのコピーは、親から子へのコピーは自由に行なうことができるものの、孫へのコピーを行なうことはできない。

【0 0 0 9】

【発明が解決しようとする課題】

そのような事情からも、音楽情報や画像情報をデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0 0 1 0】

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権限のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権限を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

【0 0 1 1】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムを提供することである。

【0 0 1 2】

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供することである。

【0 0 1 3】

【課題を解決するための手段】

請求項 1 記載のデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、コンテンツデータ供給装置は、外部との間でデータを授受するため

の第 1 のインターフェース部と暗号化コンテンツデータの通信ごとに更新される第 1 の共通鍵を生成する第 1 のセッションキー発生部と、ユーザの端末に対応して予め定められた第 1 の公開暗号化鍵により第 1 の共通鍵を暗号化して第 1 のインターフェース部に与えるためのセッションキー暗号化部と、第 1 の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、暗号化コンテンツデータを復号するためのコンテンツキーを、セッションキー復号部により復号されたデータを鍵データとして暗号化するための第 1 のライセンスデータ暗号処理部と、第 1 のライセンスデータ暗号処理部の出力を第 2 の共通鍵でさらに暗号化して第 1 のインターフェース部に与え配信するための第 2 のライセンスデータ暗号処理部とを備え、各端末は、外部との間でデータを授受するための第 2 のインターフェース部と、暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、配信データ解読部は、第 1 の公開暗号化鍵によって暗号化されたデータを復号化するための第 1 の秘密復号鍵を保持する第 1 の鍵保持部と、第 1 の公開暗号化鍵によって暗号化された第 1 の共通鍵を受けて、復号処理するための第 1 の復号処理部と、第 2 の公開暗号化鍵を保持するための第 2 の鍵保持部と、第 2 の公開暗号化鍵を、第 1 の共通鍵に基づいて暗号化し、第 2 のインターフェース部に出力するための第 1 の暗号化処理部と、第 2 のライセンスデータ暗号処理部からの暗号化されたコンテンツキーを受け、第 2 の共通鍵に基づいて復号化するための第 2 の復号処理部と、第 2 の復号処理部の出力を受けて、格納するための第 1 の記憶部と、第 2 の公開暗号化鍵によって暗号化されたデータを復号化するための第 2 の秘密復号鍵を保持する第 3 の鍵保持部と、第 1 の記憶部に格納されたデータに基づいて、第 2 の秘密復号鍵によりコンテンツキーを復号するための第 3 の復号処理部とを備える。

【 0 0 1 4 】

請求項 2 記載のデータ配信システムは、請求項 1 記載のデータ配信システムの構成に加えて、配信データ解読部は、端末に着脱可能なメモリカードであり、第 1 の公開暗号化鍵は、メモリカードの種類に対応して予め定められた鍵であり、第 2 の公開暗号化鍵は、メモリカードごとに異なる。

【 0 0 1 5 】

請求項 3 記載のデータ配信システムは、請求項 2 記載のデータ配信システムの構成に加えて、第 2 および第 3 の復号処理部は、コンテンツデータ供給装置において第 2 の公開暗号化鍵で暗号化され、さらに第 2 の共通鍵で暗号化されて、コンテンツキーとともに配信されるライセンス情報データを第 2 のインターフェース部を介して受け、第 2 の共通鍵および第 2 の秘密復号鍵に基づいて復号し、配信データ解読部は、復号されたライセンス情報データを格納する第 2 の記憶部をさらに備える。

【 0 0 1 6 】

請求項 4 記載のデータ配信システムは、請求項 3 記載のデータ配信システムの構成に加えて、第 1 の共通鍵と第 2 の共通鍵とは、暗号化コンテンツデータの通信の際に、第 1 のセッションキー発生部により生成された同一の鍵データである。

【 0 0 1 7 】

請求項 5 記載のデータ配信システムは、請求項 4 記載のデータ配信システムの構成に加えて、第 1 の記憶部は、コンテンツキーに基づいて復号できる暗号化コンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読部は、外部から指示される再生動作モードに応じて、第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第 1 の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第 3 の復号処理部からのコンテンツキーを受けて、第 3 の共通鍵に基づいて暗号化して出力し、第 1 の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第 3 の共通鍵を生成する第 2 のセッションキー発生部と、配信データ解読部からの第 3 の共通鍵により暗号化されたコンテンツキーを受けて復号して抽出し、第 1 の記憶部から出力された暗号化コンテンツデータをコンテンツキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

【 0 0 1 8 】

請求項 6 記載のデータ配信システムは、請求項 5 記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第 3 の公開暗号化鍵で暗号化処理を行なうための第 2 の暗号化処理部とをさらに含み、第 2 の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第 3 の共通鍵に基づいて暗号化されて他の端末の側から送信される第 3 の公開暗号化鍵を復号して抽出し、第 2 の暗号化処理部は、移動動作モードが指定されるのに応じて、コンテンツキーおよびライセンス情報データを第 3 の公開暗号化鍵で暗号化し、第 1 の暗号化処理部は、第 2 の暗号化処理部の出力を受けて、第 3 の共通鍵に基づいて暗号化して第 2 のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第 2 の記憶部に格納されているライセンス情報データを消去し、第 1 の記憶部は、移動動作モードが指定されるのに応じて、暗号化コンテンツデータを第 2 のインターフェース部に与える。

【 0 0 1 9 】

請求項 7 記載のデータ配信システムは、請求項 5 記載のデータ配信システムの構成に加えて、記配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第 1 の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第 2 のインターフェース部に与える。

【 0 0 2 0 】

請求項 8 記載のデータ配信システムは、請求項 3 記載のデータ配信システムの構成に加えて、配信データ解読部は、第 2 の共通鍵を生成するための第 3 のセッションキー発生部と、第 3 のセッションキー発生部の出力を暗号化して第 2 のインターフェース部に与えることが可能な第 3 の暗号化処理部とをさらに含む。

【 0 0 2 1 】

請求項 9 記載のデータ配信システムは、請求項 8 記載のデータ配信システムの構成に加えて、第 1 の記憶部は、コンテンツキーに基づいて復号できる暗号化コ

ンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読部は、外部から指示される再生動作モードに応じて、第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第 3 の暗号処理部は、第 4 の公開暗号化鍵により第 3 のセッションキー発生部の出力を暗号化して第 2 のインターフェース部に与え、第 1 の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第 3 の復号処理部からのコンテンツキーを受けて、第 3 の共通鍵に基づいて暗号化して出力し、第 1 の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第 3 の共通鍵を生成する第 2 のセッションキー発生部と、第 4 の公開暗号化鍵を配信データ解読部に与える公開鍵保持部と、第 4 の公開暗号化鍵で暗号化された第 2 の共通鍵を復号可能な公開鍵復号部と、配信データ解読部からの第 3 の共通鍵により暗号化されたコンテンツキーを受けて復号して抽出し、第 1 の記憶部から出力された暗号化コンテンツデータをコンテンツキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

【 0 0 2 2 】

請求項 1 0 記載のデータ配信システムは、請求項 9 記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第 3 の公開暗号化鍵で暗号化処理を行なうための第 2 の暗号化処理部とをさらに含み、第 2 の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第 3 の共通鍵に基づいて暗号化されて他の端末の側から送信される第 3 の公開暗号化鍵を復号して抽出し、第 2 の暗号化処理部は、移動動作モードが指定されるのに応じて、コンテンツキーおよびライセンス情報データを第 3 の公開暗号化鍵で暗号化し、第 1 の暗号化処理部は、第 2 の暗号化処理部の出力を受けて、第 3 の共通鍵に基づいて暗号化して第 2 のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第 2 の記憶部に格納されているライセンス情

報データを消去し、第 1 の記憶部は、移動動作モードが指定されるのに応じて、暗号化コンテンツデータを第 2 のインターフェース部に与える。

【0 0 2 3】

請求項 1 1 記載のデータ配信システムは、請求項 9 記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第 1 の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第 2 のインターフェース部に与える。

【0 0 2 4】

請求項 1 2 記載のデータ配信システムは、請求項 1 記載のデータ配信システムの構成に加えて、第 1 のインターフェース部と第 2 のインターフェース部とは、携帯電話網により接続され、コンテンツデータ供給装置は、

第 1 の公開暗号鍵に基づいて、ユーザの認証を行なう。

【0 0 2 5】

請求項 1 3 記載のデータ配信システムは、請求項 1 記載のデータ配信システムの構成に加えて、第 1 のインターフェース部は、端末と直接接続可能なコネクタ部を含む。

【0 0 2 6】

請求項 1 4 記載のデータ配信システムは、請求項 2 記載のデータ配信システムの構成に加えて、第 1 のインターフェース部は、メモリーカードと直接接続可能な接続部を含む。

【0 0 2 7】

【発明の実施の形態】

[実施の形態 1]

[システムの全体構成]

図 1 は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【0 0 2 8】

なお、以下では携帯電話網を介して、デジタル音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物情報データ、たとえば画像情報等の著作物情報データを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

【0029】

図1を参照して、著作権の存在する音楽情報を管理する配信サーバ10は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリアである携帯電話会社20に、このような暗号化データを与える。一方、認証サーバ12は、音楽データの配信を求めてアクセスしてきたユーザが正規のユーザであるか否かの認証を行う。

【0030】

携帯電話会社20は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ10に中継する。配信サーバ10は、配線リクエストがあると、認証サーバ12によりユーザが正規のユーザであることを確認し、要求された音楽情報をさらに暗号化したうえで、携帯電話会社20の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

【0031】

図1においては、たとえば携帯電話ユーザ1の携帯電話100には、携帯電話100により受信された暗号化された音楽データを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話100中の音楽再生部（図示せず）に与えるための着脱可能なメモリカード110が装着される構成となっている。

【0032】

さらに、たとえばユーザ1は、携帯電話100に接続したヘッドホン130等を介してこのような再生された音楽データを聴取することが可能である。

【0033】

以下では、このような配信サーバ10と認証サーバ12と配信キャリア（携帯電話会社）20とを併せて、音楽サーバ30と総称することにする。

【 0 0 3 4 】

また、このような音楽サーバ 3 0 から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

【 0 0 3 5 】

このような構成とすることで、まず、メモリカード 1 1 0 を購入していない正規のユーザでないものは、音楽サーバ 3 0 からの配信データを受取って再生することが困難な構成となる。

【 0 0 3 6 】

しかも、配信キャリア 2 0 において、たとえば 1 曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア 2 0 が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【 0 0 3 7 】

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【 0 0 3 8 】

このとき、たとえばメモリカード 1 1 2 を有するユーザ 2 が、自己の携帯電話 1 0 2 により、音楽サーバ 3 0 から直接音楽データの配信を受けることは可能である。しかしながら、相当量の情報量を有する音楽データ等をユーザ 2 が直接音楽サーバ 3 0 から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該音楽データの配信を受けているユーザ 1 から、その音楽情報をコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

【 0 0 3 9 】

しかしながら、著作権者の権利保護の観点からは、自由な音楽データのコピーを放任することはシステム構成上許されない。

【 0 0 4 0 】




図 1 に示した例では、ユーザ 1 が受信した音楽データを、デジタル音楽データそのものおよび当該音楽データを再生可能とするために必要な情報とともに、ユーザ 2 に対してコピーさせる場合を音楽データの「移動」と呼ぶ。この場合、ユーザ 1 は、再生のために必要な情報（再生情報）ごとユーザ 2 にコピーさせるため、情報の移動を行なった後には、ユーザ 1 においては音楽データの再生を行なうことは不可能とする必要がある。ここで、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたがって暗号化されたコンテンツデータを復号可能なコンテンツキー（「ライセンスキー」とも称する）と、著作権保護に関わる情報であるライセンス ID データやユーザ ID データ等のライセンス情報とを意味する。

【 0 0 4 1 】

これに対して、音楽データ（コンテンツデータ）のみを暗号化されたままの状態、ユーザ 2 にコピーさせることを音楽情報の「複製」と呼ぶこととする。

【 0 0 4 2 】

この場合、ユーザ 2 の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされない、ユーザ 2 は、コンテンツデータを得ただけでは、音楽情報を再生させることができない。したがって、ユーザ 2 が、このような音楽情報の再生を望む場合は、改めて音楽サーバ 3 0 からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよい、ユーザ 2 が直接音楽サーバ 3 0 からすべての情報の配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

【 0 0 4 3 】

たとえば、携帯電話 1 0 0 および 1 0 2 が、P H S（Personal Handy Phone）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ 1 からユーザ 2 への一括した情報の移転（移動）や、コンテンツデータのみの転送（複製）を行なうことが可能である。

【 0 0 4 4 】

図 1 に示したような構成においては、暗号化して配信される音楽データ（コン

テンツデータ) をユーザ側で再生可能とするためにシステム上必要とされるのは、第 1 には、通信における暗号化キー (鍵) を配送するための方式であり、さらに第 2 には、配信データを暗号化する方式そのものであり、さらに、第 3 には、このようにして配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

【 0 0 4 5 】

[暗号／復号キーの構成]

図 2 は、図 1 に示した情報配信システムにおいて使用される通信のためのキーデータ (鍵データ) 等の特性をまとめて説明するための図である。

【 0 0 4 6 】

まず、図 1 に示した構成において、メモ리카ード 1 0 0 内のデータ処理を管理するための鍵としては、メモ리카ードという媒体の種類に固有であり、かつ、メモ리카ードの種類等を個別に特定するための情報を含む秘密復号鍵 $K_{media}(n)$ (n : 自然数) と、メモ리카ードごとに異なる公開暗号化鍵 $K_{Pcard}(n)$ と、公開暗号化鍵 $K_{Pcard}(n)$ により暗号化されたデータを復号するための秘密復号鍵 $K_{card}(n)$ とがある。

【 0 0 4 7 】

ここで、鍵 $K_{card}(n)$ や鍵 $K_{Pcard}(n)$ の表記中の自然数 n は、各メモ리카ードを区別するための番号を表わす。

【 0 0 4 8 】

すなわち、公開暗号化鍵 $K_{Pcard}(n)$ で暗号化されたデータは、各メモ리카ードごとに存在する秘密復号鍵 $K_{card}(n)$ で復号可能である。したがって、メモ리카ードにおける配信データの授受にあたっては、基本的には、後に説明するように 3 つの暗号鍵 $K_{media}(n)$ 、 $K_{card}(n)$ 、 $K_{Pcard}(n)$ が用いられることになる。

【 0 0 4 9 】

さらに、メモ리카ード外とメモ리카ード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有な公開暗号化鍵 $K_{Pmedia}(n)$ と、公開暗号化鍵 $K_{Pmedia}(n)$ により暗号化されたデータを復号化するた

めの秘密復号鍵 $K_{media}(n)$ と、各通信ごと、たとえば、サーバ 30 へのユーザのアクセスごとにサーバ 30、携帯電話機 100 または 102 において生成される共通鍵 K_s が用いられる。

【0050】

ここで、共通鍵 K_s は、たとえば、ユーザが音楽サーバ 30 に対して 1 回のアクセスを行なうごとに発生する構成として、1 回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、たとえば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

【0051】

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵 K_s を「セッションキー」とも呼ぶことにする。

【0052】

したがって、共通鍵 K_s は各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

【0053】

また、配信されるべきデータについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵である K_c （以下、ライセンスキーと呼ぶ）があり、この共通鍵 K_c により暗号化されたコンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンス ID データ $L i c e n s e - I D$ 等が存在する。一方、携帯電話は、受信者を識別するためのユーザ ID データ $U s e r - I D$ を保持している。

【0054】

このような構成とすることで、ライセンス ID データに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザ ID データを用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

【0055】

配信データにおけるコンテンツデータ D_c は、上述のとおり、たとえば音楽情報データであり、このコンテンツデータをライセンスキー K_c で復号化可能なデータを、暗号化コンテンツデータ $[D_c] K_c$ と呼ぶ。

【0056】

ここで、 $[Y] X$ という表記は、データ Y を、鍵データ X により復号可能な暗号に変換した情報であることを示している。

【0057】**[音楽サーバ30の構成]**

図3は、図1に示した音楽サーバ30の構成を示す概略ブロック図である。音楽サーバ30は、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したデータや、ライセンスID等の配信情報を保持するための配信情報データベース304と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース302と、配信情報データベース304および課金データベース302からのデータをデータバスBS1を介して受取り、所定の暗号化処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0058】

データ処理部310は、データバスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部312と、配信制御部312に制御されて、セッションキー K_s を発生するためのセッションキー発生部314と、セッションキー発生部314より生成されたセッションキー K_s を、公開暗号化鍵 $KPmedia$ により暗号化して、データバスBS1に与えるための暗号化処理部316と、各ユーザの携帯電話においてセッションキー K_s により暗号化されたうえで送信されたデータを通信装置350およびデータバスBS1を介して受けて、復号処理を行なう復号処理部318と、復号処理部318により抽出された公開暗号化鍵 $KPcard(n)$ を用いて、ライセンスキーやライセンスID等のデータを配信制御部312に制御されて暗号化するための暗号化処理部32

0 と、暗号化処理部 3 2 0 の出力を、さらにセッションキー K_s により暗号化して、データバス BS_1 を介して通信装置 3 5 0 に与える暗号化処理部 3 2 2 とを含む。

【0059】

[端末（携帯電話機）の構成]

図 4 は、図 1 に示した携帯電話 1 0 0 の構成を説明するための概略ブロック図である。

【0060】

携帯電話 1 0 0 は、携帯電話網により無線伝送される信号を受信するためのアンテナ 1 1 0 2 と、アンテナ 1 1 0 2 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話からのデータを変調してアンテナ 1 1 0 2 に与えるための送受信部 1 1 0 4 と、携帯電話 1 0 0 の各部のデータ授受を行なうためのデータバス BS_2 と、データバス BS_2 を介して携帯電話 1 0 0 の動作を制御するためのコントローラ 1 1 0 6 と、受信者を識別するためのユーザ ID データ $User-ID$ を保持するユーザ ID 保持部 1 1 0 7 と、外部からの指示を携帯電話 1 0 0 に与えるためのタッチキー部 1 1 0 8 と、コントローラ 1 1 0 6 等から出力される情報をユーザに視覚情報として与えるためのディスプレイ 1 1 1 0 と、通常の通話動作において、データバス BS_2 を介して与えられる受信データに基づいて音声を再生するための音声再生部 1 1 1 2 と、外部との間でデータの授受を行なうためのコネクタ 1 1 2 0 と、コネクタ 1 1 2 0 からのデータをデータバス BS_2 に与え得る信号に変換し、または、データバス BS_2 からのデータをコネクタ 1 1 2 0 に与え得る信号に変換するための外部インターフェース部 1 1 2 2 とを備える。

【0061】

ここで、ユーザ ID データは、たとえばユーザの電話番号等のデータを含む。

携帯電話 1 0 0 は、さらに、サーバ 3 0 からの音楽データを復号化処理するための着脱可能なメモリカード 1 1 0 と、メモリカード 1 1 0 とデータバス BS_2 との間のデータの授受を制御するためのメモリインタフェース 1 2 0 0 と、メモリカード 1 1 0 と携帯電話の他の部分とのデータ授受にあたり、データバス BS

2 上においてやり取りされるデータを暗号化するためのセッションキー K_s を乱数等により発生するセッションキー発生部 1 5 0 2 と、セッションキー発生部 1 5 0 2 により生成されたセッションキーを暗号化して、データバス BS_2 に与えるための暗号化処理部 1 5 0 4 と、セッションキー発生部 1 5 0 2 において生成された、データバス BS_2 上のデータをセッションキー K_s により復号して出力する復号処理部 1 5 0 6 と、復号処理部 1 5 0 6 の出力を受けて、音楽データを再生するための音楽再生部 1 5 0 8 と、音楽再生部 1 5 0 8 の出力と音声再生部 1 1 1 2 の出力とを受けて、動作モードに応じて選択的に出力するための混合部 1 5 1 0 と、混合部 1 5 1 0 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1 5 1 2 と、デジタルアナログ変換部 1 5 1 2 の出力を受けて、ヘッドホン 1 3 0 と接続するための接続端子 1 5 1 4 とを含む。

【0 0 6 2】

なお、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、形態電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【0 0 6 3】

[メモ리카ードの構成]

図 5 は、図 4 に示したメモ리카ード 1 1 0 の構成を説明するための概略ブロック図である。

【0 0 6 4】

以下では、端末 1 0 0 に装着されるメモ리카ード 1 1 0 の公開暗号化キー K_{Pmedia} と、端末 1 0 2 に装着されるメモ리카ード 1 1 2 の公開暗号化キー K_{Pmedia} とを区別して、それぞれ、メモ리카ード 1 1 0 に対するものを公開暗号化キー $K_{Pmedia}(1)$ と、メモ리카ード 1 1 2 に対するものを公開暗号化キー $K_{Pmedia}(2)$ と称することにする。

【0 0 6 5】

また、これに対応して、公開暗号化キー $K_{Pmedia}(1)$ で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キー K_m

e d i a (1) と称し、公開暗号化キー K P m e d i a (2) で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キー K m e d i a (2) と称することにする。

【 0 0 6 6 】

このように、媒体固有の公開暗号化キーを区別することにより、以下の説明で明らかとなるように、メモ리카ードに複数の種類が存在する場合や、より一般的に、メモ리카ード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。

【 0 0 6 7 】

メモ리카ード 1 1 0 は、メモリアインタフェース 1 2 0 0 との間で信号を端子 1 2 0 2 を介して授受するデータバス B S 3 と、公開暗号化キー K P m e d i a (1) の値を保持し、データバス B S 3 に公開暗号化キー K P m e d i a (1) を出力するための K P m e d i a (1) 保持部 1 4 0 1 と、カード 1 1 0 に対応する秘密復号鍵 K m e d i a (1) を保持するための K m e d i a (1) 保持部 1 4 0 2 と、データバス B S 3 にメモリアインタフェース 1 2 0 0 から与えられるデータから、秘密復号鍵 K m e d i a (1) により復号処理をすることにより、セッションキー K s を抽出する復号処理部 1 4 0 4 と、公開暗号化キー K P c a r d (1) を保持するための K P c a r d (1) 保持部 1 4 0 5 と、復号処理部 1 4 0 4 により抽出されたセッションキー K s に基づいて、切換スイッチ 1 4 0 8 からの出力を暗号化してデータバス B S 3 に与えるための暗号化処理部 1 4 0 6 と、データバス B S 3 上のデータを復号処理部 1 4 0 4 により抽出されたセッションキー K s により復号処理してデータバス B S 4 に与えるための復号処理部 1 4 1 0 と、データバス B S 4 からメモ리카ードごとに異なる公開暗号化鍵 K P c a r d (n) で暗号化されているライセンスキー K c 、ライセンス I D 等のデータを格納し、データバス B S 3 からライセンスキー K c により暗号化されている暗号化コンテンツデータ [D c] K c を受けて格納するためのメモリ 1 4 1 2 とを備える。

【 0 0 6 8 】

切換えスイッチ 1 4 0 8 は、接点 P a 、 P b 、 P c を有し、接点 P a には K P

c a r d (1) 保持部 1 4 0 5 からの公開暗号化キー K P c a r d (1) が、接点 P b にはデータバス B S 5 が、接点 P c には暗号化処理部 1 4 1 4 の出力が与えられる。切換えスイッチ 1 4 0 8 は、それぞれ、接点 P a 、 P b 、 P c に与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部 1 4 0 6 に与える。

【 0 0 6 9 】

メモ리카ード 1 1 0 は、さらに、キー K c a r d (1) の値を保持するための K c a r d (1) 保持部 1 4 1 5 と、公開暗号化鍵 K P c a r d (1) により暗号化されており、かつ、メモリ 1 4 1 2 から読出されたライセンスキー K c 、ライセンス I D 等 ([K c , L i c e n s e] K c a r d (1)) を、復号処理してデータバス B S 5 に与える復号処理部 1 4 1 6 と、データの移動処理等において、相手先のメモ리카ードの公開暗号化鍵 K P c a r d (n) を復号処理部 1 4 1 0 から受けて、この相手方の公開暗号化鍵 K P c a r d (n) に基づいて、データバス B S 5 上に出力されているライセンスキー K c 、ライセンス I D 等を暗号化したうえで、切換えスイッチ 1 4 0 8 に出力するための暗号化処理部 1 4 1 4 と、データバス B S 3 を介して外部とデータの授受を行い、データバス B S 5 との間でライセンス I D データ等を受けて、メモ리카ード 1 1 0 の動作を制御するためのコントローラ 1 4 2 0 と、データバス B S 5 との間でライセンス I D データ等のデータの授受が可能なレジスタ 1 5 0 0 とを備える。

【 0 0 7 0 】

なお、図 5 において実線で囲んだ領域は、メモ리카ード 1 1 0 内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュール T R M に組込まれているものとする。

【 0 0 7 1 】

このようなモジュールは、一般にはタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

【 0 0 7 2 】

もちろん、メモリ 1 4 1 2 も含めて、モジュール T R M 内に組み込まれる構成

としてもよい。しかしながら、図 5 に示したような構成とすることで、メモリ 1 4 1 2 中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ 1 4 1 2 中のデータのみでは、音楽データを再生することは不可能であり、かつ高価なタンプルレジスタンスモジュール内にメモリ 1 4 1 2 を設ける必要がないので、製造コストが低減されるという利点がある。

【0 0 7 3】

図 6 および図 7 は、図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信動作を説明するための第 1 および第 2 のフローチャートである。

【0 0 7 4】

図 6 および図 7 においては、ユーザ 1 が、メモリカード 1 1 0 を用いることで、音楽サーバ 3 0 から音楽データの配信を受ける場合の動作を説明している。

【0 0 7 5】

まず、ユーザ 1 の携帯電話機 1 0 0 から、ユーザによりキーボード 1 1 0 8 のキーボタンの操作等によって、配信リクエストがなされる（ステップ S 1 0 0）。

【0 0 7 6】

カード 1 1 0 においては、この配信リクエストに応じて、K P m e d i a (1) 保持部 1 4 0 1 から、公開暗号化キー K P m e d i a (1) をサーバ 3 0 に対して送信する（ステップ S 1 0 2）。

【0 0 7 7】

サーバ 3 0 では、カード 1 1 0 から転送された配信リクエストならびにキー K P m e d i a (1) を受信すると（ステップ S 1 0 4）、受信したキー K P m e d i a (1) に基づいて、認証サーバ 1 2 に対して照会を行ない、正規ユーザからのアクセスの場合は次の処理に移行し（ステップ S 1 0 6）、正規ユーザでない場合には、処理を終了する（ステップ S 1 5 4）。

【0 0 7 8】

照会の結果、正規ユーザであることが確認されると、サーバ 3 0 では、セッションキー発生部 3 1 4 が、セッションキー K s を生成する。さらに、サーバ 3 0 内の暗号化処理部 3 1 6 が、受信したキー K P m e d i a (1) により、このセ

セッションキー K_s を暗号化してデータ $[K_s] K_{media}(1)$ を生成する（ステップ S 1 0 8）。

【0 0 7 9】

続いて、サーバ 3 0 は、データ $[K_s] K_{media}(1)$ をデータバス B S 1 に与える。通信装置 3 5 0 は、暗号化処理部 3 1 6 からの暗号化データ $[K_s] K_{media}(1)$ を、通信網を通じて、携帯電話機 1 0 0 のメモリカード 1 1 0 に対して送信する（ステップ S 1 1 0）。

【0 0 8 0】

携帯電話機 1 0 0 が、データ $[K_s] K_{media}(1)$ を受信すると（ステップ S 1 1 2）、メモリカード 1 1 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス B S 3 に与えられた受信データを、復号処理部 1 4 0 4 が、キーデータ $K_{media}(1)$ により復号処理することにより、セッションキーデータ K_s を復号し抽出する（ステップ S 1 1 4）。

【0 0 8 1】

続いて、配信動作においては、切換スイッチ 1 4 0 8 は、接点 P a が閉じる状態が選択されているので、暗号化処理部 1 4 0 6 は、接点 P a を介して $K P c a r d(1)$ 保持部 1 4 0 5 から与えられる公開暗号化鍵 $K P c a r d(1)$ （メモリカード 1 1 0 に対する公開暗号化鍵）を、セッションキー K_s により暗号化し（ステップ S 1 1 6）、データ $[K P c a r d(1)] K_s$ を生成する（ステップ S 1 1 8）。

【0 0 8 2】

携帯電話機 1 0 0 は、暗号化処理部 1 4 0 6 により暗号化されたデータ $[K P c a r d(1)] K_s$ をサーバ 3 0 に対して送信する（ステップ S 1 2 0）。

【0 0 8 3】

サーバ 3 0 では、通信装置 3 5 0 によりデータ $[K P c a r d(1)] K_s$ が受信され（ステップ S 1 2 2）、データバス B S 1 に与えられたデータ $[K P c a r d(1)] K_s$ を復号処理部 3 1 8 が、セッションキー K_s により復号処理して、キーデータ $K P c a r d(1)$ を復号抽出する（ステップ S 1 2 4）。

【0 0 8 4】

続いて、配信制御部 3 1 2 は、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ等を含むライセンス情報データ L i c e n s e を生成する（ステップ S 1 2 6）。

【0 0 8 5】

さらに、サーバ 3 0 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、通信装置 3 5 0 を介して、メモリカード 1 1 0 に送信する（ステップ S 1 2 8）。

【0 0 8 6】

携帯電話機 1 0 0 がデータ [D c] K c を受信すると（ステップ S 1 3 0）、メモリカード 1 1 0 においては、受信したデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する（ステップ S 1 3 2）。

【0 0 8 7】

一方、サーバ 3 0 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し（ステップ S 1 3 4）、暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのキーデータ K c とライセンス情報データ L i c e n s e とを、復号処理部 3 1 8 より与えられたキーデータ K P c a r d (1) により暗号化処理する（ステップ S 1 3 6）。

【0 0 8 8】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [K c、L i c e n s e] K c a r d (1) を受取って、さらにセッションキー K s により暗号化したデータをデータバス B S 1 に与える。通信装置 3 5 0 は、暗号化処理部 3 2 2 により暗号化されたデータ [[K c, L i c e n s e] K c a r d (1)] K s をカード 1 1 0 に対して送信する。

【0 0 8 9】

携帯電話 1 0 0 がデータ [[K c, L i c e n s e] K c a r d (1)] K s を受信すると（ステップ S 1 4 2）、カード 1 1 0 においては、復号処理部 1 4 1 0 がセッションキー K s により復号処理を行ない、データ [K c, L i c e n s e] K c a r d (1) を抽出し、メモリ 1 4 1 2 に格納する（ステップ S 1 4 6）。

【0090】

さらに、カード110においては、コントローラ1420により制御されて、復号処理部1416が、メモリ1412に格納されたデータ[Kc, License] Kcard (1)を復号し、復号されたライセンス情報データLicenseを、レジスタ1500に格納する(ステップ148)。

【0091】

以上のような動作により、メモリカード自身が、セッションキーKsを送る側(サーバ30)に、公開暗号化キーKPmedia (1)を送信した上で、配信を受けることができ、メモリカード110は、音楽情報を再生可能な状態となる。以下では、メモリカードが音楽情報を再生可能な状態となっていることを、「メモリカード110は、状態SAにある」と呼ぶことにする。一方、メモリカードが音楽情報を再生不可能な状態となっていることを、「メモリカード110は、状態SBにある」と呼ぶことにする。

【0092】

さらに、メモリカード110からサーバ30へは、配信受理が通知され、サーバ30で配信受理を受信すると(ステップS150)、課金データベース302にユーザ1の課金データが格納され(ステップS152)、処理が終了する(ステップS154)。

【0093】

図8は、携帯電話100内において、メモリカード110に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0094】

図8を参照して、携帯電話のキーボード1108等からのユーザ1の指示により、再生リクエストがメモリカード110に対して出力される(ステップS200)。

【0095】

カード110においては、この再生リクエストに応じて、コントローラ1420は、レジスタ1500に保持されるライセンス情報データに基づいて、復号可

能なデータに対するリクエストであるかを判断し（ステップS 2 0 2）、復号可能と判断した場合は、K P m e d i a (1) 保持部 1 4 0 1 から、公開暗号化キー K P m e d i a (1) を携帯電話 1 0 0 に対して送信する（ステップS 2 0 4）。一方、復号不可能と判断した場合は、処理を終了する（ステップS 2 3 0）。

【0 0 9 6】

復号可能と判断され、カード 1 1 0 から公開暗号化キー K P m e d i a (1) が送信された場合、携帯電話 1 0 0 では、カード 1 1 0 からのキー K P m e d i a (1) を受信すると（ステップS 2 0 6）、K s 発生部 1 5 0 2 においてセッションキー K s を生成し、暗号化処理部 1 5 0 4 が、キー K P m e d i a (1) により、セッションキー K s を暗号化してデータ [K s] K P m e d i a (1) を生成し、データバス B S 2 を介して、カード 1 1 0 に対して送信する（ステップS 2 0 8）。

【0 0 9 7】

メモリカード 1 1 0 は、データバス B S 2 を介して、携帯電話機により生成され、かつ暗号化されたセッションキー K s を受け取り、キーデータ K m e d i a (1) により復号し、セッションキー K s を抽出する（ステップS 2 1 0）。

【0 0 9 8】

続いて、メモリカード 1 1 0 は、メモリ 1 4 1 2 から、暗号化されているデータ [K c , L i c e n s e] K c a r d (1) を読出し、復号処理部 1 4 1 6 が復号処理を行なう（ステップS 2 1 2）。

【0 0 9 9】

キー K c a r d (1) により、メモリ 1 4 1 2 から読み出されたデータを復号可能な場合（ステップS 2 1 4）、ライセンスキー K c が抽出される（ステップS 2 1 6）。一方、復号不可能の場合、処理は終了する（ステップS 2 3 2）。

【0 1 0 0】

メモリ 1 4 1 2 から読み出されたデータを復号可能な場合（ステップS 2 1 4）は、レジスタ 1 5 0 0 内のライセンス情報データのうち、再生回数に関するデ

ータが変更される（ステップ S 2 1 8）。

【0 1 0 1】

続いて、抽出したセッションキー K_s により、ライセンスキー K_c を暗号化し（ステップ S 2 2 0）、暗号化されたライセンスキー $[K_c] K_s$ をデータベース BS_2 に与える（ステップ S 2 2 2）。

【0 1 0 2】

携帯電話機 1 0 0 の復号処理部 1 5 0 6 は、セッションキー K_s により復号化処理を行なうことにより、ライセンスキー K_c を取得する（ステップ S 2 2 4）。

【0 1 0 3】

続いて、メモ리카ード 1 1 0 は、暗号化されたコンテンツデータ $[D_c] K_c$ をメモリ 1 4 1 2 から読出し、データベース BS_2 に与える（ステップ S 2 2 6）。

【0 1 0 4】

携帯電話機の音楽再生部 1 5 0 8 は、暗号化されたコンテンツデータ $[D_c] K_c$ を、抽出されたキーデータ K_c により復号処理して平文の音楽データを生成し（ステップ S 2 2 8）、コンテンツデータを再生して混合部 1 5 1 0 に与える（ステップ S 2 3 0）。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップ S 2 3 2）。

【0 1 0 5】

このような構成とすることで、メモ리카ード自身が、セッションキー K_s を送る側（携帯電話機 1 0 0）に、公開暗号化キー $K_{Pmedia}(1)$ を送信した上で、再生動作を行うことが可能となる。

【0 1 0 6】

図 9 および図 1 0 は、2 つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 および第 2 のフローチャートである。

【0 1 0 7】

まず、携帯電話機 1 0 2 が送信側であり、携帯電話機 1 0 0 が受信側であるものとする。また、携帯電話機 1 0 2 にも、メモリカード 1 1 0 と同様の構成を有するメモリカード 1 1 2 が装着されているものとする。

【0 1 0 8】

携帯電話機 1 0 2 は、まず、自身の側のメモリカード 1 1 2 および携帯電話 1 0 0 に対して、移動リクエストまたは複製リクエストを出力する（ステップ S 3 0 0）。

【0 1 0 9】

カード 1 1 2 は、これに応じて、メモリ 1 4 1 2 内のデータ [D c] K c を読み出して、メモリカード 1 1 0 に対して出力し（ステップ S 3 0 2）、一方、携帯電話 1 0 0 は、携帯電話 1 0 2 からリクエストを受信して（ステップ S 3 0 1）、メモリカード 1 1 0 では、データ [D c] K c をメモリ 1 4 1 2 に格納する（ステップ S 3 0 4）。

【0 1 1 0】

続いて、携帯電話 1 0 2 および 1 0 0 においては、ステップ S 3 0 0 において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップ S 3 0 6、ステップ S 3 0 6'）、「移動リクエスト」である場合、カード 1 1 2 は、公開暗号化キー K P m e d i a (2) を携帯電話機 1 0 2 に対して送信し（ステップ S 3 0 8）、携帯電話 1 0 2 は、キー K P m e d i a (2) を受信する（ステップ S 3 1 2）。一方、カード 1 1 0 は、「移動リクエスト」である場合、公開暗号化キー K P m e d i a (1) を携帯電話機 1 0 0 に出力し（ステップ S 3 0 8'）、携帯電話 1 0 0 は、公開暗号化キー K P m e d i a (1) を携帯電話機 1 0 2 に対して送信する（ステップ S 3 1 0）。

【0 1 1 1】

携帯電話機 1 0 2 が、キー K P m e d i a (1) およびキー K P m e d i a (2) を受信すると（ステップ S 3 1 2、ステップ S 3 1 2'）、携帯電話機 1 0 2 においては、セッションキー発生回路 1 5 0 2 は、セッションキー K s を生成し（ステップ S 3 0 3）、公開暗号化キー K P m e d i a (1) およびキー K P

media (2) を用いて、暗号化処理部 1 5 0 4 がセッションキー K s を暗号化する (ステップ S 3 1 4)。

【0 1 1 2】

携帯電話機 1 0 2 は、データバス B S 2 を介して、カード 1 1 2 に対しては暗号化されたセッションキー [K s] K P media (2) を伝達し、カード 1 1 2 においては、キーデータ K media (2) によりセッションキー K s を復号抽出する (ステップ S 3 2 8)。

【0 1 1 3】

さらに、携帯電話機 1 0 2 は、暗号化されたセッションキー [K s] K P media (1) を携帯電話機 1 0 0 に対して送信する (ステップ S 3 1 6)。携帯電話機 1 0 0 は、データ [K s] K P media (1) を受信すると (ステップ S 3 1 8)、カード 1 1 0 に伝達し、カード 1 1 0 は、復号処理部 1 4 0 4 が復号して、セッションキー K s を受理する (ステップ S 3 2 0)。

【0 1 1 4】

カード 1 1 0 においては、セッションキー K s によりカード 1 1 0 の公開暗号化キー K P card (1) を暗号化して (ステップ S 3 2 2)、携帯電話機 1 0 0 から携帯電話機 1 0 2 に対して暗号化されたデータ [K P card (1)] K s を送信する (ステップ S 3 2 4)。携帯電話機 1 0 2 は、データ [K P card (1)] K s を受信し (ステップ S 3 2 6)、かつ、カード 1 1 2 によるキー K s の受理が完了すると (ステップ S 3 2 8)、カード 1 1 2 においては、カード 1 1 0 から送信された暗号化データ [K P card (1)] K s をセッションキー K s により復号化して、カード 1 1 0 の公開暗号化キー K P card (1) を復号抽出する (ステップ S 3 3 0)。

【0 1 1 5】

続いて、カード 1 1 2 においては、メモリ 1 4 1 2 からカード 1 1 2 の公開暗号化キー K card (2) により暗号化されているライセンスキー K c、ライセンス情報データ L i c e n s e が読出される (ステップ S 3 3 2)。

【0 1 1 6】

続いて、カード 1 1 2 の復号処理部 1 4 1 6 が、キーデータ K card (2)

により、ライセンスキー K_c 、データ $L i c e n s e$ を復号処理する（ステップ $S 3 3 4$ ）。

【0 1 1 7】

カード 1 1 2 のコントローラ 1 4 2 0 は、このようにして復号されたライセンス情報データ $L i c e n s e$ の値を、レジスタ 1 5 0 0 内のデータ値と置換する（ステップ $S 3 3 6$ ）。

【0 1 1 8】

さらに、カード 1 1 2 の暗号化処理部 1 4 1 4 は、復号処理部 1 4 1 0 において抽出されたカード 1 1 0 における公開暗号化キー $K P c a r d (1)$ により、キーデータ K_c 、データ $L i c e n s e$ とを暗号化する（ステップ $S 3 3 8$ ）。

【0 1 1 9】

カード 1 1 2 の暗号化処理部 1 4 1 4 により暗号化されたデータは、切換スイッチ 1 4 0 8（接点 P_c が閉じている）を介して、さらに、暗号化処理部 1 4 0 6 に与えられ、暗号化処理部 1 4 0 6 は、データ $[K_c, L i c e n s e] K c a r d (1)$ をセッションキー K_s により暗号化してデータ $[[K_c, L i c e n s e] K c a r d (1)] K_s$ を生成する（ステップ $S 3 4 0$ ）。

【0 1 2 0】

続いて、メモリカード 1 1 2 は、携帯電話機 1 0 2 に対してデータ $[[K_c, L i c e n s e] K c a r d (1)] K_s$ を出力し（ステップ $S 3 4 2$ ）、携帯電話機 1 0 2 はデータ $[[K_c, L i c e n s e] K c a r d (1)] K_s$ を携帯電話機 1 0 0 に対して送信する（ステップ $S 3 4 4$ ）。

【0 1 2 1】

携帯電話機 1 0 0 が受信したデータ $[[K_c, L i c e n s e] K c a r d (1)] K_s$ は（ステップ $S 3 4 6$ ）、メモリカード 1 1 0 に対して伝達され、メモリカード 1 1 0 の復号処理部 1 4 1 0 は、暗号化されたデータ $[[K_c, L i c e n s e] K c a r d (1)] K_s$ を復号して、データ $[K_c, L i c e n s e] K c a r d (1)$ を受理する（ステップ $S 3 4 8$ ）。

【0 1 2 2】

カード 1 1 0 においては、復号処理部 1 4 1 0 により、セッションキー K_s に

基づいて復号化処理されたデータをメモリ 1 4 1 2 に格納する（ステップ S 3 5 0）。さらに、カード 1 1 0 においては、復号処理部 1 4 1 6 が、キーデータ K c a r d (1) に基づいて、データ [K c , L i c e n s e] K c a r d (1) を復号し、復号されたライセンス情報データ L i c e n s e をレジスタ 1 5 0 0 に格納する（ステップ S 3 5 2）。

【0 1 2 3】

復号されたライセンス情報データ L i c e n s e のレジスタ 1 5 0 0 への格納が終了すると、メモリカード 1 1 0 は携帯電話 1 0 0 に移動受理を通知し、携帯電話 1 0 0 は、携帯電話 1 0 2 に対して移動受理を送信する（ステップ S 3 5 4）。

【0 1 2 4】

携帯電話 1 0 2 は、携帯電話 1 0 0 からの移動受理を受信すると、メモリカード 1 1 2 に対してこれを転送し、メモリカード 1 1 2 は、これに応じて、レジスタ 1 5 0 0 に格納されたライセンス情報データ 1 5 0 0 を消去する（ステップ 3 5 8）。

【0 1 2 5】

一方、携帯電話 1 0 2 では、移動受理が受信されたことに応じて、ディスプレイ 1 1 1 0 上に、ユーザ 2 に対して、メモリカード 1 1 2 のメモリ 1 4 1 2 内に格納されている移動データに対応する記憶データの消去を行なうかを問うメッセージを表示する。これに応じて、ユーザ 2 は、キーボード 1 1 0 8 からこのメッセージに対する回答を入力する（ステップ S 3 6 0）。

【0 1 2 6】

レジスタ 1 5 0 0 内のデータの消去が完了し（ステップ S 3 5 8）、かつ、上記メッセージに対する回答の入力が行なわれると（ステップ S 3 6 0）、メモリカード 1 1 2 内のコントローラ 1 4 2 0 は、メモリ 1 4 1 2 内のデータの消去を行なうかの判断を行う（ステップ S 3 6 2）。

【0 1 2 7】

メモリ 1 4 1 2 内の該当データの消去が指示されている場合（ステップ S 3 6 2）、コントローラ 1 4 2 0 により制御されて、メモリ 1 4 1 2 内のデータ [D

c] K c およびデータ [K c , L i c e n s e] K c a r d (2) が消去され (ステップ S 3 6 4) 、処理が終了する (ステップ S 3 7 4) 。

【 0 1 2 8 】

一方、メモリ 1 4 1 2 内の該当データの消去が指示されていない場合 (ステップ S 3 6 2) 、処理は終了する (ステップ S 3 7 4) 。この場合、メモリ 1 4 1 2 内には、データ [D c] K c およびデータ [K c , L i c e n s e] K c a r d (2) が残っていることになるが、レジスタ 1 5 0 0 内にライセンス情報データが存在しないため、ユーザ 2 は、再度、サーバ 3 0 から再生情報を配信してもらわない限り、音楽データの再生を行なうことはできない。すなわち、カード 1 1 2 は「状態 S B」となる。カード 1 1 0 においては、暗号化されたコンテンツデータ以外にも、ライセンスキーデータ K c 、ライセンス情報データが移動されているので、カード 1 1 0 は「状態 S A」となっている。

【 0 1 2 9 】

一方、ステップ S 3 0 6 ' において、「複製リクエスト」が与えられていると判断された場合は、携帯電話機 1 0 0 から携帯電話機 1 0 2 に対して複製受取が送信される (ステップ S 3 7 0) 。携帯電話機 1 0 2 において、複製受取を受信すると (ステップ S 3 7 2) 、処理が終了する (ステップ S 3 7 4) 。

【 0 1 3 0 】

このような構成とすることで、メモリカード自身が、セッションキー K s を送る側 (携帯電話機 1 0 0) に、公開暗号化キー K P m e d i a (1) および K P m e d i a (2) を送信した上で、移動動作を行うこと、および複製動作を行なうことが可能となる。

【 0 1 3 1 】

[実施の形態 2]

実施の形態 2 のデータ配信システムにおいては、実施の形態 1 のデータ配信システムの構成と異なって、配信サーバ、携帯電話機およびメモリカードの各々が、独自のセッションキーを生成する構成となっていることを 1 つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーをキー K s とし、一方のメモリカード 1 2 0 の発生するセッションキーをキー K s 1 とし、メ

メモリカード 1 2 0 と同様の構成を有する他方のメモリカード 1 2 2 の発生するセッションキーをキー K s 2 とする。

【0 1 3 2】

すなわち、実施の形態 2 のデータ配信システムにおいては、システムを構成する機器の各々が、自身でセッションキーを生成し、データを受け取るとき、言い換えるとデータの送信先になっている場合には、相手方（送信元）に対して、まず、セッションキーを配送する。送信元は、この送信先から配送されたセッションキーでデータを暗号化し、この暗号化データを送信する。送信先では、自身で生成したセッションキーにより、受け取ったデータを復号化するという構成を 1 つの特徴とするものである。

【0 1 3 3】

また、上記のような動作を実現するために、再生動作において、携帯電話機側がメモリカードの生成するセッションキーを受け取るための公開暗号化キーを K P p とし、このキー K P p で暗号化されたデータを復号化できる秘密復号キーをキー K p とする。

【0 1 3 4】

図 1 1 は、実施の形態 2 のメモリカード 1 2 0 に対応した音楽サーバ 3 1 の構成を示す概略ブロック図である。図 3 に示した音楽サーバ 3 0 の構成と異なる点は、データ処理部 3 1 0 における暗号化処理部 3 2 2 は、K s 発生部 3 1 4 からのセッションキー K s に基づいてではなく、携帯電話機に装着されたメモリカードからセッションキー K s により暗号化されて送信され、復号処理部 3 1 8 により復号抽出されたセッションキー、たとえば、キー K s 1 に基づいて、暗号化処理部 3 2 0 の出力をさらに暗号化して、データバス B S 1 を介して通信装置 3 5 0 に与える点である。

【0 1 3 5】

音楽サーバ 3 1 のその他の点は、図 3 に示した実施の形態 1 の音楽サーバ 3 0 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 1 3 6】

図 1 2 は、実施の形態 2 における携帯電話機 1 0 1 の構成を説明するための概略ブロック図である。

【0 1 3 7】

図 4 に示した携帯電話機 1 0 0 の構成と異なる点は、まず、メモ리카ード 1 2 0 が装着されていること以外に、携帯電話機 1 0 1 は、公開暗号化キー K P p を保持して、再生動作時にキー K P p をデータベース B S 2 に出力する K P p 保持部 1 5 2 4 を備える構成となっていることである。

【0 1 3 8】

さらに、携帯電話機 1 0 1 は、秘密復号キー K p を保持する K p 保持部 1 5 2 0 と、この K p 保持部 1 5 2 0 から与えられるキー K p に基づいて、データベース B S 2 を介してメモ리카ード 1 2 0 から与えられるキー K P p で暗号化されたセッションキー K s 1 を復号し抽出する復号処理部 1 5 2 2 とをさらに備える構成となっている。しかも、暗号化処理部 1 5 0 4 は、この復号処理部 1 5 2 2 から与えられるセッションキー K s 1 により、K s 発生部 1 5 0 2 からの自身のセッションキー K s を暗号化してデータベース B S 2 に出力する。

【0 1 3 9】

携帯電話機 1 0 1 のその他の点は、図 4 に示した実施の形態 1 の携帯電話機 1 0 0 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 1 4 0】

図 1 3 は、本発明の実施の形態 2 のメモ리카ード 1 2 0 の構成を説明するための概略ブロック図であり、実施の形態 1 の図 5 と対比される図である。

【0 1 4 1】

メモ리카ード 1 2 0 の構成が、メモ리카ード 1 1 0 の構成と異なる点は、まず、メモ리카ード 1 2 0 は、このカード独自のセッションキー K s 1 を発生するセッションキー K s 1 発生部 1 4 3 2 を備えることである。

【0 1 4 2】

さらに、メモ리카ード 1 2 0 は、セッションキー発生回路 1 4 3 2 で生成されたセッションキー K s 1 を、暗号化してデータベース B S 3 に与えるための暗号化

処理部 1 4 3 0 を備える。

【 0 1 4 3 】

これに応じて、メモリカード 1 2 0 は、さらに、移動動作において、相手方（移動先）の公開暗号化キー $KPmedia(n)$ を受けて保持する $KPmedia$ 受理部 1 4 0 3 と、この $KPmedia$ 受理部 1 4 0 3 の出力と、再生動作においてデータバス $BS3$ を介して携帯電話機 1 0 1 から与えられる公開暗号化キー KPp とを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ 1 4 3 6 を備える。切換えスイッチ 1 4 3 6 は、接点 Pi および Ph とを有し、接点 Pi はデータバス $BS3$ と、接点 Ph は $KPmedia$ 受理部 1 4 0 3 とそれぞれ結合する。暗号化処理部 1 4 3 0 は、切換えスイッチ 1 4 3 6 から与えられるキー $KPmedia(n)$ またはキー KPp のいずれかにより、 $Ks1$ 発生部 1 4 3 2 からのセッションキー $Ks1$ を暗号化して、データバス $BS3$ に与える。

【 0 1 4 4 】

すなわち、切換えスイッチ 1 4 3 6 は、配信動作のとき、および移動動作において移動先となっているときは、未使用状態であり、再生動作の時は、接点 Pi の側に閉じており、移動動作において移動元となっているときは、接点 Ph の側に閉じている。

【 0 1 4 5 】

メモリカード 1 2 0 は、さらに、接点 Pe 、 Pf および Pg を有し、復号処理部 1 4 0 4 から与えられる配信サーバからのセッションキー Ks と、 $Ks1$ 発生部 1 4 3 2 の出力と、データバス $BS4$ から与えられる携帯電話機 1 0 1 からのセッションキー Ks とを受けて、動作モードに応じていずれか 1 つを選択的に出力する切換えスイッチ 1 4 3 5 を備える。接点 Pe には復号処理部 1 4 0 4 からの出力が、接点 Pf には $Ks1$ 発生部 1 4 3 2 の出力が、接点 Pg にはデータバス $BS4$ がそれぞれ結合している。したがって、暗号化処理部 1 4 0 6 と復号処理部 1 4 1 0 は、この切換えスイッチ 1 4 3 5 から与えられるキーに基づいて、それぞれ、暗号化処理および復号処理を行う。

【 0 1 4 6 】

すなわち、切換えスイッチ 1 4 3 5 は、配信動作の場合に配信サーバ 3 1 からのセッションキーの抽出を行なうときは、接点 P e の側に閉じており、配信動作の場合に配信サーバ 3 1 からの暗号化されたライセンスキー K c、ライセンス情報データについてキー K s 1 による復号を行なうときは、接点 P f の側に閉じている。切換えスイッチ 1 4 3 5 は、再生動作において復号処理を行うときは、接点 P f の側に閉じており、再生動作において暗号化処理を行うときは、接点 P g の側に閉じている。切換えスイッチ 1 4 3 5 は、移動動作において移動元となっている場合に復号処理を行うときは、接点 P f の側に閉じており、移動動作において移動元となっている場合に暗号化処理を行うときは、接点 P g の側に閉じている。切換えスイッチ 1 4 3 5 は、移動動作において移動先となっている場合に移動元のセッションキーを受け取るときは、接点 P e の側に閉じており、移動動作において移動先となっている場合にライセンスキー K c およびライセンス情報データを受け取るときは、接点 P f の側に閉じている。

【0 1 4 7】

メモリカード 1 2 0 は、さらに、接点 P a、P b、P c および P d を有し、K s 1 発生部 1 4 3 2 から与えられる自身のセッションキー K s 1 と、K P c a r d 保持部 1 4 0 5 の出力と、データベース B S 5 から与えられるライセンスキー K c と、暗号化処理部 1 4 1 4 から与えられ、相手方の公開暗号化キー K P c a r d (n) により暗号化されたライセンスキー K c およびライセンス情報データを受けて、動作モードに応じていずれか 1 つを選択的に出力する切換えスイッチ 1 4 0 9 を、切換えスイッチ 1 4 0 8 の替わりに備える。

【0 1 4 8】

接点 P a には K s 1 発生部 1 4 3 2 からの出力が、接点 P b には K P c a r d (1) 保持部 1 4 0 5 の出力が、接点 P c にはデータベース B S 5 が、接点 P d には暗号化処理部 1 4 1 4 の出力が、それぞれ結合している。したがって、暗号化処理部 1 4 0 6 は、この切換えスイッチ 1 4 0 9 から与えられるデータに対して、それぞれ、暗号化処理を行う。

【0 1 4 9】

すなわち、切換えスイッチ 1 4 0 9 は、配信動作において、配信先となってい

る場合にサーバ 3 1 に自身の公開暗号化キー K P c a r d (1) や自身のセッションキー K s 1 を送信するときは、順次、接点 P b の側および接点 P a の側に閉じる。切換えスイッチ 1 4 0 9 は、再生動作のときは、接点 P c の側に閉じており、移動動作において移動元となっているときは、接点 P d の側に閉じている。切換えスイッチ 1 4 0 9 は、移動動作において移動先となっている場合にも移動元に自身の公開暗号化キー K P c a r d (1) や自身のセッションキー K s 1 を送信するときは、順次、接点 P b の側および接点 P a の側に閉じる。

【 0 1 5 0 】

図 1 4 および図 1 5 は、図 1 3 で説明したメモリカード 1 2 0 を用いた配信動作を説明するための第 1 および第 2 のフローチャートである。

【 0 1 5 1 】

図 6 および図 7 においても、ユーザ 1 が、メモリカード 1 1 0 を用いることで、音楽サーバ 3 0 から音楽データの配信を受ける場合の動作を説明している。

【 0 1 5 2 】

まず、ユーザ 1 の携帯電話機 1 0 1 から、ユーザによりキーボード 1 1 0 8 のキーボタンの操作等によって、配信リクエストがなされる（ステップ S 1 0 0 ）。

【 0 1 5 3 】

カード 1 2 0 においては、この配信リクエストに応じて、K P m e d i a (1) 保持部 1 4 0 1 から、公開暗号化キー K P m e d i a (1) をサーバ 3 1 に対して送信する（ステップ S 1 0 2 ）。さらに、カード 1 2 0 においては、K s 1 発生部 1 4 3 2 によりセッションキー K s 1 が生成される（ステップ S 1 0 9 ）。

【 0 1 5 4 】

サーバ 3 1 では、カード 1 2 0 から転送された配信リクエストならびにキー K P m e d i a (1) を受信すると（ステップ S 1 0 4 ）、受信したキー K P m e d i a (1) に基づいて、認証サーバ 1 2 に対して照会を行ない、正規ユーザからのアクセスの場合は次の処理に移行し（ステップ S 1 0 6 ）、正規ユーザでない場合には、処理を終了する（ステップ S 1 5 4 ）。

【0 1 5 5】

照会の結果、正規ユーザであることが確認されると、サーバ 3 1 では、セッションキー発生部 3 1 4 が、セッションキー K_s を生成する。さらに、サーバ 3 1 内の暗号化処理部 3 1 6 が、受信したキー $K_{Pmedia}(1)$ により、このセッションキー K_s を暗号化してデータ $[K_s] K_{media}(1)$ を生成する（ステップ S 1 0 8）。

【0 1 5 6】

続いて、サーバ 3 1 は、データ $[K_s] K_{media}(1)$ をデータバス BS 1 に与える。通信装置 3 5 0 は、暗号化処理部 3 1 6 からの暗号化データ $[K_s] K_{media}(1)$ を、通信網を通じて、携帯電話機 1 0 1 のメモリカード 1 2 0 に対して送信する（ステップ S 1 1 0）。

【0 1 5 7】

携帯電話機 1 0 1 が、データ $[K_s] K_{media}(1)$ を受信すると（ステップ S 1 1 2）、メモリカード 1 2 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス BS 3 に与えられた受信データを、復号処理部 1 4 0 4 が、キーデータ $K_{media}(1)$ で復号処理することにより、セッションキーデータ K_s を復号し抽出する（ステップ S 1 1 4）。

【0 1 5 8】

続いて、配信動作においては、切換スイッチ 1 4 0 9 は、接点 P a または P b が順次閉じる状態が選択されるので、暗号化処理部 1 4 0 6 は、接点 P a を介してセッションキー発生部 1 4 3 2 から与えられるセッションキー K_{s1} と接点 P b を介して $K_{Pcard}(1)$ 保持部 1 4 0 5 から与えられる公開暗号化鍵 $K_{Pcard}(1)$ （メモリカード 1 2 0 に対する公開暗号化鍵）とを、セッションキー K_s により暗号化し（ステップ S 1 1 6）、データ $[K_{Pcard}(1), K_{s1}] K_s$ を生成する（ステップ S 1 1 8）。

【0 1 5 9】

携帯電話機 1 0 1 は、暗号化処理部 1 4 0 6 により暗号化されたデータ $[K_{Pcard}(1), K_{s1}] K_s$ をサーバ 3 1 に対して送信する（ステップ S 1 2 0）。

【0160】

サーバ31では、通信装置350によりデータ[KPcard(1)、Ks1] Ksが受信され(ステップS122)、データベースBS1に与えられたデータ[KPcard(1)、Ks1] Ksを復号処理部318が、セッションキーKsにより復号処理して、キーデータKPcard(1)およびセッションキーKs1を復号抽出する(ステップS124)。

【0161】

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する(ステップS126)。

【0162】

さらに、サーバ31は、暗号化コンテンツデータ[Dc] Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード120に送信する(ステップS128)。

【0163】

携帯電話機101がデータ[Dc] Kcを受信すると(ステップS130)、メモリカード120においては、受信したデータ[Dc] Kcをそのままメモリ1412に格納する(ステップS132)。

【0164】

一方、サーバ31は、ライセンスキーKcを配信情報データベース304より取得し(ステップS134)、暗号化処理部320は、配信制御部312からのキーデータKcとライセンス情報データLicenseとを、復号処理部318より与えられたキーデータKPcard(1)により暗号化処理する(ステップS136)。

【0165】

暗号化処理部322は、暗号化処理部320により暗号化されたデータ[Kc、License] Kcard(1)を受取って、さらに、メモリカード120からのセッションキーKs1により暗号化したデータをデータベースBS1に与える。通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc

, License] Kcard (1)] Ks1 をカード 120 に対して送信する。

【0166】

携帯電話 101 がデータ [[Kc, License] Kcard (1)] Ks1 を受信すると (ステップ S142)、カード 120 においては、復号処理部 1410 が接点 Pf を介して Ks1 発生部 1432 から与えられるセッションキー Ks1 により復号処理を行ない、データ [Kc, License] Kcard (1) を抽出し、メモリ 1412 に格納する (ステップ S146)。

【0167】

さらに、カード 120 においては、コントローラ 1420 により制御されて、復号処理部 1416 が、メモリ 1412 に格納されたデータ [Kc, License] Kcard (1) を復号し、復号されたライセンス情報データ License を、レジスタ 1500 に格納する (ステップ 148)。

【0168】

以上のような動作により、メモ리카ード 120 自身が、暗号化コンテンツデータを送る側 (サーバ 31) に、公開暗号化キー KPmedia (1) およびセッションキー Ks1 を送信した上で、配信を受けることができ、メモ리카ード 120 は、音楽情報を再生可能な状態となる。

【0169】

さらに、メモ리카ード 120 からサーバ 31 へは、配信受理が通知され、サーバ 31 で配信受理を受信すると (ステップ S150)、課金データベース 302 にユーザ 1 の課金データが格納され (ステップ S152)、処理が終了する (ステップ S154)。

【0170】

図 16 および図 17 は、携帯電話 101 内において、メモ리카ード 120 に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明する第 1 および第 2 のフローチャートである。

【0171】

図 16 および図 17 を参照して、携帯電話のキーボード 1108 等からのユー

ザ 1 の指示により、再生リクエストがメモリカード 1 2 0 に対して出力される（ステップ S 2 0 0）。

【0 1 7 2】

カード 1 2 0 においては、この再生リクエストに応じて、コントローラ 1 4 2 0 は、レジスタ 1 5 0 0 に保持されるライセンス情報データに基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップ S 2 0 2）、復号可能と判断した場合は、再生可能通知を携帯電話 1 0 1 に対して送信する（ステップ S 2 4 0）。一方、復号不可能と判断した場合は、処理を終了する（ステップ S 2 8 0）。

【0 1 7 3】

復号可能と判断され、カード 1 2 0 から再生可能通知が送信された場合、携帯電話 1 0 1 では、公開暗号化キー K P p をカード 1 2 0 に送信し（ステップ S 2 4 2）、K s 発生部 1 5 0 2 においてセッションキー K s を生成する（ステップ S 2 4 4）。

【0 1 7 4】

一方、メモリカード 1 2 0 も、セッションキー K s 1 を生成する（ステップ S 2 4 0）。メモリカード 1 2 0 は、さらに、データバス B S 2 を介して携帯電話機から受けとったキー K P p によりセッションキー K s 1 を暗号化し（ステップ S 2 4 8）、生成されたデータ [K s 1] K p を携帯電話 1 0 1 に対して送信する（ステップ S 2 5 0）。

【0 1 7 5】

携帯電話 1 0 1 では、メモリカード 1 2 0 からのデータ [K s 1] K p を受信すると、復号処理部 1 5 2 2 が、キー K p により復号化してメモリカード 1 2 0 で生成したセッションキー K s 1 を抽出する（ステップ S 2 5 2）。続いて、携帯電話 1 0 1 の暗号化処理部 1 5 0 4 は、携帯電話 1 0 1 で生成したセッションキー K s をキー K s 1 により暗号化して、データ [K s] K s 1 を生成し（ステップ S 2 5 4）、このデータ [K s] K s 1 をメモリカード 1 2 0 に対して送信する（ステップ S 2 5 6）。

【0 1 7 6】

メモ리카ード 1 2 0 は、データベース B S 2 を介して、携帯電話機により生成され、かつ暗号化されたセッションキー K s を受け取り、セッションキー K s 1 により復号し、携帯電話 1 0 1 で生成したセッションキー K s を抽出する（ステップ S 2 5 8）。

【0 1 7 7】

続いて、メモ리카ード 1 2 0 は、メモリ 1 4 1 2 から、暗号化されているデータ [K c, L i c e n s e] K c a r d (1) を読出し、復号処理部 1 4 1 6 が復号処理を行なう（ステップ S 2 6 0）。

【0 1 7 8】

キー K c a r d (1) により、メモリ 1 4 1 2 から読み出されたデータを復号可能な場合（ステップ S 2 6 2）、ライセンスキー K c が抽出される（ステップ S 2 6 4）。一方、復号不可能の場合、処理は終了する（ステップ S 2 8 0）。

【0 1 7 9】

メモリ 1 4 1 2 から読み出されたデータを復号可能な場合は、さらに、レジスタ 1 5 0 0 内のライセンス情報データのうち、再生回数に関するデータが変更される（ステップ S 2 6 6）。

【0 1 8 0】

続いて、メモ리카ード 1 2 0 においては、暗号化処理部 1 4 0 6 が、抽出したセッションキー K s により、ライセンスキー K c を暗号化し（ステップ S 2 6 8）、暗号化されたライセンスキー [K c] K s をデータベース B S 2 に与える（ステップ S 2 7 0）。

【0 1 8 1】

携帯電話機 1 0 1 の復号処理部 1 5 0 6 は、セッションキー K s により復号化処理を行なうことにより、ライセンスキー K c を取得する（ステップ S 2 7 2）。

【0 1 8 2】

続いて、メモ리카ード 1 2 0 は、暗号化されたコンテンツデータ [D c] K c をメモリ 1 4 1 2 から読出し、データベース B S 2 に与える（ステップ S 2 7 4）。

。

【0183】

携帯電話機の音楽再生部 1 5 0 8 は、暗号化されたコンテンツデータ [D c] K c を、抽出されたキーデータ K c により復号処理して平文の音楽データを生成し（ステップ S 2 7 6）、コンテンツデータを再生して混合部 1 5 1 0 に与える（ステップ S 2 7 6）。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップ S 2 3 2）。

【0184】

このような構成とすることで、メモリカード自身および携帯電話自身が、それぞれセッションキー K s 1 または K s を生成し、これにより暗号化されたデータの授受を行なった上で、再生動作を行うことが可能となる。

【0185】

図 1 8 および図 1 9 は、2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 および第 2 のフローチャートである。

【0186】

まず、携帯電話 1 0 1 と同様の構成を有する携帯電話機 1 0 3 が送信側であり、携帯電話機 1 0 1 が受信側であるものとする。また、携帯電話機 1 0 3 にも、メモリカード 1 2 0 と同様の構成を有するメモリカード 1 2 2 が装着されているものとする。

【0187】

携帯電話機 1 0 3 は、まず、自身の側のメモリカード 1 2 2 および携帯電話 1 0 1 に対して、移動リクエストまたは複製リクエストを出力する（ステップ S 3 0 0）。

【0188】

カード 1 2 2 は、これに応じて、メモリ 1 4 1 2 内のデータ [D c] K c を読み出して、メモリカード 1 2 0 に対して出力し（ステップ S 3 0 2）、一方、携帯電話 1 0 1 は、携帯電話機 1 0 3 からのリクエストを受信し（ステップ S 3 0

1)、メモリカード 1 2 0 では、データ [D c] K c をメモリ 1 4 1 2 に格納する (ステップ S 3 0 4)。

【0 1 8 9】

続いて、携帯電話 1 0 3 および 1 0 1 においては、ステップ S 3 0 0 において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され (ステップ S 3 0 6、ステップ S 3 0 6')、「移動リクエスト」である場合、カード 1 2 0 は、公開暗号化キー K P m e d i a (1) を携帯電話機 1 0 1 に出力し (ステップ S 3 0 8)、携帯電話 1 0 1 は、公開暗号化キー K P m e d i a (1) を携帯電話機 1 0 3 に対して送信する (ステップ S 3 1 0)。

【0 1 9 0】

携帯電話機 1 0 3 が、キー K P m e d i a (1) を受信し (ステップ S 3 1 2)、メモリカード 1 2 2 に転送すると (ステップ S 3 1 3)、メモリカード 1 2 2 の K s 2 発生回路 1 4 3 2 は、セッションキー K s 2 を生成し (ステップ S 3 1 4)、公開暗号化キー K P m e d i a (1) を用いて、暗号化処理部 1 4 3 0 がセッションキー K s 2 を暗号化する (ステップ S 3 1 5)。

【0 1 9 1】

携帯電話機 1 0 3 は、暗号化されたセッションキー [K s 2] K P m e d i a (1) を携帯電話機 1 0 1 に対して送信する (ステップ S 3 1 6)。携帯電話機 1 0 1 は、データ [K s 2] K P m e d i a (1) を受信すると (ステップ S 3 1 8)、カード 1 2 0 に伝達し、カード 1 2 0 は、復号処理部 1 4 0 4 が復号して、セッションキー K s 2 を受理する (ステップ S 3 2 0)。

【0 1 9 2】

カード 1 2 0 においては、セッションキー K s 2 によりカード 1 2 0 の公開暗号化キー K P c a r d (1) およびセッションキー K s 1 を暗号化して (ステップ S 3 2 2)、携帯電話機 1 0 1 から携帯電話機 1 0 3 に対して暗号化されたデータ [K P c a r d (1)、K s 1] K s 2 を送信する (ステップ S 3 2 4)。携帯電話機 1 0 3 は、データ [K P c a r d (1)、K s 1] K s 2 を受信し (ステップ S 3 2 6)、カード 1 2 2 に転送する。

【0193】

カード 1 2 2 においては、復号処理部 1 4 1 0 が、カード 1 2 0 から送信された暗号化データ [K P c a r d (1)、K s 1] K s 2 をセッションキー K s 2 により復号化して、カード 1 2 0 の公開暗号化キー K P c a r d (1)、セッションキー K s 1 を復号抽出する (ステップ S 3 3 0)。

【0194】

続いて、カード 1 2 2 においては、メモリ 1 4 1 2 からカード 1 2 2 の公開暗号化キー K c a r d (2) により暗号化されているライセンスキー K c、ライセンス情報データ L i c e n s e が読出される (ステップ S 3 3 2)。

【0195】

続いて、カード 1 2 2 の復号処理部 1 4 1 6 が、キーデータ K c a r d (2) により、ライセンスキー K c、データ L i c e n s e を復号処理する (ステップ S 3 3 4)。

【0196】

カード 1 2 2 のコントローラ 1 4 2 0 は、このようにして復号されたライセンス情報データ L i c e n s e の値を、レジスタ 1 5 0 0 内のデータ値と置換する (ステップ S 3 3 6)。

【0197】

さらに、カード 1 2 2 の暗号化処理部 1 4 1 4 は、復号処理部 1 4 1 0 において抽出されたカード 1 2 0 における公開暗号化キー K P c a r d (1) により、キーデータ K c、データ L i c e n s e とを暗号化する (ステップ S 3 3 8)。

【0198】

カード 1 2 2 の暗号化処理部 1 4 1 4 により暗号化されたデータは、切換スイッチ 1 4 0 9 (接点 P d が閉じている) を介して、さらに、暗号化処理部 1 4 0 6 に与えられ、メモリカード 1 2 2 の暗号化処理部 1 4 0 6 は、データ [K c, L i c e n s e] K c a r d (1) をセッションキー K s 1 により暗号化してデータ [[K c, L i c e n s e] K c a r d (1)] K s 1 を生成する (ステップ S 3 4 0)。

【0199】

続いて、メモリカード 122 は、携帯電話機 103 に対してデータ [[Kc, License] Kcard (1)] Ks1 を出力し (ステップ S342)、携帯電話機 103 はデータ [[Kc, License] Kcard (1)] Ks1 を携帯電話機 101 に対して送信する (ステップ S344)。

【0200】

携帯電話機 101 が受信したデータ [[Kc, License] Kcard (1)] Ks1 は (ステップ S346)、メモリカード 120 に対して伝達され、メモリカード 120 の復号処理部 1410 は、暗号化されたデータ [[Kc, License] Kcard (1)] Ks1 を復号して、データ [Kc, License] Kcard (1) を受理する (ステップ S348)。

【0201】

カード 120 においては、復号処理部 1410 により、セッションキー Ks1 に基づいて復号化処理されたデータ [Kc, License] Kcard (1) をメモリ 1412 に格納する (ステップ S350)。さらに、カード 120 においては、復号処理部 1416 が、キーデータ Kcard (1) に基づいて、データ [Kc, License] Kcard (1) を復号し、復号されたライセンス情報データ License をレジスタ 1500 に格納する (ステップ S352)。

。

【0202】

以後の移動動作における処理ならびに複製動作におけるメモリカード 120 および 122 の処理は、図 9 および図 10 で説明した実施の形態 1 のメモリカード 110、112 等の処理と同様であるので、その説明は繰り返さない。

【0203】

このような構成とすることで、移動元および移動先のメモリカード自身が、セッションキーをそれぞれ生成した上で、移動動作を行うこと、および複製動作を行なうことが可能となる。

【0204】

したがって、データバス上で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティーが一層

向上するという効果がある。

【0205】

しかも、以上のような構成を用いることで、たとえば、メモリカード 122 からメモリカード 120 へのデータの移動を、上述したようなセッションキー発生回路 1502 を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインターフェース機器により行うことも可能となり、ユーザの利便性が一層向上するという効果がある。

【0206】

ここで、移動時には、再生情報内の再生回数を制限するライセンス情報データについては、メモリ 1412 に記録されたライセンス情報データを、レジスタ 1500 にて再生の都度修正された再生回数を記録したライセンス情報データに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

【0207】

[実施の形態 3]

実施の形態 3 のデータ配信システムにおいては、ユーザは、配信キャリアである携帯電話会社 20 から暗号化コンテンツデータの配信を受けるのではなく、たとえば、街頭などに設置されているコンテンツデータ販売機から暗号化コンテンツデータの供給を受ける構成となっていることを 1 つの特徴とする。

【0208】

図 20 は、このような実施の形態 3 のデータ配信システムの構成を説明するための概念図である。なお、携帯電話機 100 およびメモリカード 110 の構成は実施の形態 1 で説明したものと同様であるので、その説明は繰り返さない。

【0209】

図 20 を参照して、コンテンツデータ販売機 2000 は、ユーザに対して配信作業における案内等を出力するためのディスプレイ 2002 と、ユーザから指示を入力するためのキーボード 2004 と、料金投入口 2006 と、携帯電話 10

0 とコネクタ 1 1 2 0 を介してデータの授受を行うための外部コネクタ 2 0 1 0 とを備える。さらに、コンテンツデータ販売機 2 0 0 0 は、携帯電話網等の通信路を介して、販売記録等を管理するための管理サーバ 2 2 0 0 と接続している。

【0 2 1 0】

図 2 1 は、実施の形態 3 のコンテンツデータ販売機 2 0 0 0 の構成を示す概略ブロック図である。コンテンツデータ販売機 2 0 0 0 は、上述したように、ディスプレイ 2 0 0 2 と、キーボード 2 0 0 4 と、料金投入口 2 0 0 6 からの投入金を受ける料金受理部 2 0 2 0 と、外部コネクタ 2 0 1 0 と、コネクタ 2 0 1 0 とデータベースとの間に設けられるインターフェース部 2 0 1 2 と、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したデータや、ライセンス情報データ等の配信情報を保持するための配信情報データベース 3 0 4 と、管理サーバ 2 2 0 0 との間で情報の授受をするための通信装置 3 6 0 と、配信情報データベース 3 0 4 および管理サーバ 2 2 0 0 からのデータをデータベース B S 1 を介して受取り、所定の暗号化処理を行なうためのデータ処理部 2 1 0 0 とを備える。

【0 2 1 1】

データ処理部 2 1 0 0 中は、実施の形態 1 と同様に、データベース B S 1 上のデータに応じて、データ処理部 2 1 0 0 の動作を制御するための配信制御部 3 1 2 と、配信制御部 3 1 2 に制御されて、セッションキー K s を発生するためのセッションキー発生部 3 1 4 と、セッションキー発生部 3 1 4 より生成されたセッションキー K s を、カード媒体に固有な公開暗号化鍵 K P m e d i a (n) により暗号化して、データベース B S 1 に与えるための暗号化処理部 3 1 6 と、各ユーザの携帯電話においてセッションキー K s により暗号化されたうえでコネクタ 2 0 1 0 から与えられたデータをデータベース B S 1 を介して受けて、復号処理を行なう復号処理部 3 1 8 と、復号処理部 3 1 8 により抽出された公開暗号化鍵 K P c a r d (n) を用いて、ライセンス情報データを配信制御部 3 1 2 に制御されて暗号化するための暗号化処理部 3 2 0 と、暗号化処理部 3 2 0 の出力を、さらにセッションキー K s により暗号化して、データベース B S 1 を介してコネクタ 2 0 1 0 に与える暗号化処理部 3 2 2 とを含む。

【0 2 1 2】

図 2 2 および図 2 3 は、図 2 0 および図 2 1 で説明したデータ配信システムにおける配信動作を説明するための第 1 および第 2 のフローチャートである。

【0 2 1 3】

図 2 2 および図 2 3 においては、ユーザ 1 が、メモリカード 1 1 0 を用いることで、コンテンツデータ販売機 2 0 0 0 から音楽データの配信を受ける場合の動作を説明している。

【0 2 1 4】

まず、ユーザが、コンテンツデータ販売機 2 0 0 0 のキーボード 2 0 0 4 のキーボタンの操作等によって、配信リクエストを指示する（ステップ S 4 0 0）。販売機 2 0 0 0 は、カード 1 1 0 に対して公開暗号化キー K P m e d i a (1) の送信依頼を出力する（ステップ S 4 0 2）。

【0 2 1 5】

カード 1 1 0 においては、この公開暗号化キー K P m e d i a (1) の送信依頼に応じて、K P m e d i a (1) 保持部 1 4 0 1 から、公開暗号化キー K P m e d i a (1) を携帯電話機 1 0 0 に対して出力する（ステップ S 4 0 6）。

【0 2 1 6】

携帯電話 1 0 0 が販売機 2 0 0 0 にキー K P m e d i a (1) を送信し（ステップ S 4 0 8）、販売機 2 0 0 0 が、カード 1 1 0 から転送されたキー K P m e d i a (1) を受信すると（ステップ S 4 1 0）、ディスプレイ 2 0 0 2 を介してユーザに料金投入を案内し、料金徴収を行なう（ステップ S 4 1 2）。続いて、販売機 2 0 0 0 は、セッションキー発生部 3 1 4 が、セッションキー K s を生成する。さらに、販売機 2 0 0 0 内の暗号化処理部 3 1 6 が、受信したキー K P m e d i a (1) により、このセッションキー K s を暗号化してデータ [K s] K m e d i a (1) を生成する（ステップ S 4 1 4）。

【0 2 1 7】

続いて、販売機 2 0 0 0 は、データ [K s] K m e d i a (1) をデータバス B S 1 に与え、コネクタ 2 0 1 0 から出力する（ステップ S 4 1 6）。携帯電話機 1 0 0 は、このデータ [K s] K m e d i a (1) を受信すると、メモリカード 1 1 0 に転送する（ステップ S 4 1 8）。

【0 2 1 8】

メモ리카ード 1 1 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス B S 3 に与えられた受信データ [K s] K m e d i a (1) を、復号処理部 1 4 0 4 が、キーデータ K m e d i a (1) により復号処理することにより、セッションキーデータ K s を復号し抽出する（ステップ S 4 2 0）。

【0 2 1 9】

続いて、配信動作においては、切換スイッチ 1 4 0 8 は、接点 P a が閉じる状態が選択されているので、暗号化処理部 1 4 0 6 は、接点 P a を介して K P c a r d (1) 保持部 1 4 0 5 から与えられる公開暗号化鍵 K P c a r d (1) を、セッションキー K s により暗号化し（ステップ S 4 2 2）、データ [K P c a r d (1)] K s を生成する（ステップ S 4 2 4）。

【0 2 2 0】

携帯電話機 1 0 0 は、暗号化処理部 1 4 0 6 により暗号化されたデータ [K P c a r d (1)] K s を販売機 2 0 0 0 に対して送信する（ステップ S 4 2 6）。

【0 2 2 1】

販売機 2 0 0 0 では、コネクタ 2 0 1 0 を介してデータ [K P c a r d (1)] K s が受信され（ステップ S 4 2 8）、データバス B S 1 に与えられたデータ [K P c a r d (1)] K s を復号処理部 3 1 8 が、セッションキー K s により復号処理して、キーデータ K P c a r d (1) を復号抽出する（ステップ S 4 3 0）。

【0 2 2 2】

続いて、配信制御部 3 1 2 は、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ等を含むライセンス情報データ L i c e n s e を生成する（ステップ S 4 3 2）。

【0 2 2 3】

さらに、販売機 2 0 0 0 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、コネクタ 2 0 1 0 を介して、携帯電話機 1 0 0 に送信する（ステップ S 4 3 4）。

【0 2 2 4】

携帯電話機 1 0 0 がデータ [D c] K c を受信すると（ステップ S 4 3 6）、メモリカード 1 1 0 においては、受信したデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する（ステップ S 4 3 8）。

【0 2 2 5】

一方、販売機 2 0 0 0 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し（ステップ S 4 4 0）、暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのキーデータ K c とライセンス情報データ L i c e n s e とを、復号処理部 3 1 8 より与えられたキーデータ K P c a r d (1) により暗号化処理する（ステップ S 4 4 2）。

【0 2 2 6】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [K c、L i c e n s e] K c a r d (1) を受取って、さらにセッションキー K s により暗号化したデータをデータバス B S 1 に与え、暗号化処理部 3 2 2 により暗号化されたデータ [[K c, L i c e n s e] K c a r d (1)] K s がカード 1 1 0 に対して送信される（ステップ S 4 4 6）。

【0 2 2 7】

携帯電話 1 0 0 がデータ [[K c, L i c e n s e] K c a r d (1)] K s を受信すると（ステップ S 4 4 8）、カード 1 1 0 においては、復号処理部 1 4 1 0 がセッションキー K s により復号処理を行ない、データ [K c, L i c e n s e] K c a r d (1) を抽出し、メモリ 1 4 1 2 に格納する（ステップ S 4 5 2）。

【0 2 2 8】

さらに、カード 1 1 0 においては、コントローラ 1 4 2 0 により制御されて、復号処理部 1 4 1 6 が、メモリ 1 4 1 2 に格納されたデータ [K c, L i c e n s e] K c a r d (1) を復号し、復号されたライセンス情報データ L i c e n s e を、レジスタ 1 5 0 0 に格納する（ステップ S 4 5 8）。

【0 2 2 9】

以上のような動作により、メモリカード自身が、セッションキー K s を送る側

(販売機 2 0 0 0) に、公開暗号化キー K P m e d i a (1) を送信した上で、配信を受けることができ、メモリカード 1 1 0 は、音楽情報を再生可能な状態となる。

【0 2 3 0】

さらに、メモリカード 1 1 0 から販売機 2 0 0 0 へは、携帯電話機 1 0 0 を介して配信受理が通知され (ステップ S 4 6 0)、販売機 2 0 0 0 で配信受理を受信すると (ステップ S 4 6 2)、管理サーバに販売記録が送信され (ステップ S 4 6 4)、処理が終了する (ステップ S 4 6 6)。

【0 2 3 1】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等の配信を受けることができる。

【0 2 3 2】

[実施の形態 3 の変形例]

実施の形態 3 のデータ配信システムにおいては、メモリカード 1 1 0 は、携帯電話 1 0 0 を介して、コンテンツデータ販売機 2 0 0 0 から暗号化コンテンツデータの配信を受ける構成であった。

【0 2 3 3】

しかしながら、図 2 1 に示した販売機 2 0 0 0 の構成において、コネクタ 2 0 1 0 の代わりに、メモリカード 1 1 0 との間のインターフェースのためのメモリスロットを設ける構成とすれば、携帯電話 1 0 0 を介することなく、メモリカード 1 1 0 と販売機 2 0 0 0 とが直接データの授受を行うことが可能である。

【0 2 3 4】

図 2 4 は、このような実施の形態 3 の変形例のコンテンツデータ販売機 2 0 0 1 の構成を示す概念図である。図 2 0 に示した実施の形態 3 の販売機 2 0 0 0 の構成と異なる点は、外部コネクタ 2 0 1 0 の代わりに、メモリカードを挿入できるカードスロット 2 0 3 0 が設けられ、このカードスロット 2 0 3 0 がインターフェース部 2 0 1 2 を介して、データバス B S 1 とデータの授受をする構成となっている点である。

【0 2 3 5】

図 2 5 および図 2 6 は、実施の形態 3 の変形例のデータ配信システムにおける配信動作を説明するための第 1 および第 2 のフローチャートである。

【0 2 3 6】

図 2 2 および図 2 3 に示した実施の形態 3 の配信動作とは、携帯電話 1 0 0 を介さずに、メモ리카ード 1 1 0 と販売機 2 0 0 1 がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

【0 2 3 7】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

【0 2 3 8】

しかも、メモ리카ードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、音楽データの再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

【0 2 3 9】

[実施の形態 4]

図 2 7 は、実施の形態 4 のコンテンツデータ販売機 3 0 0 0 の構成を説明するための概略ブロック図である。図 2 1 に示したコンテンツデータ販売機 2 0 0 0 の構成と異なる点は、対象となるメモ리카ードが実施の形態 2 のメモ리카ード 1 2 0 であり、かつ使用される端末が携帯電話 1 0 1 である点、およびこれに対応して、データ処理部 2 1 0 0 における暗号化処理部 3 2 2 は、K s 発生部 3 1 4 からのセッションキー K s に基づいてではなく、携帯電話機に装着されたメモ리카ードからセッションキー K s により暗号化されて送信され、復号処理部 3 1 8 により復号抽出されたセッションキー、たとえば、キー K s 1 に基づいて、暗号化処理部 3 2 0 の出力をさらに暗号化して、データバス B S 1 を介してインターフェース部 2 0 1 2 およびコネクタ 2 0 1 0 に与える点である。

【0 2 4 0】

コンテンツデータ販売機 3 0 0 0 のその他の点は、図 2 1 に示した実施の形態 3 のコンテンツデータ販売機 2 0 0 0 の構成の構成と同様であるので、同一部分

には同一符号を付してその説明は繰り返さない。

【0 2 4 1】

また、携帯電話 1 0 1 およびメモリカード 1 1 0 の構成も実施の形態 2 で説明したものと同様であるので、その説明も繰り返さない。

【0 2 4 2】

図 2 8 および図 2 9 は、図 2 7 で説明したデータ配信システムにおける配信動作を説明するための第 1 および第 2 のフローチャートである。

【0 2 4 3】

図 2 8 および図 2 9 においては、ユーザ 1 が、メモリカード 1 2 0 を用いることで、コンテンツデータ販売機 3 0 0 0 から音楽データの配信を受ける場合の動作を説明している。

【0 2 4 4】

まず、ユーザが、コンテンツデータ販売機 3 0 0 0 のキーボード 2 0 0 4 のキーボタンの操作等によって、配信リクエストを指示する（ステップ S 5 0 0）。販売機 2 0 0 0 は、カード 1 1 0 に対して公開暗号化キー K P m e d i a (1) の送信依頼を出力する（ステップ S 5 0 2）。

【0 2 4 5】

カード 1 2 0 においては、この公開暗号化キー K P m e d i a (1) の送信依頼に応じて、K P m e d i a (1) 保持部 1 4 0 1 から、公開暗号化キー K P m e d i a (1) を販売機 3 0 0 0 に対して送信する（ステップ S 5 0 6）。さらに、カード 1 2 0 においては、K s 1 発生部 1 4 3 2 によりセッションキー K s 1 が生成される（ステップ S 5 1 5）。

【0 2 4 6】

携帯電話 1 0 1 が販売機 3 0 0 0 にキー K P m e d i a (1) を送信し（ステップ S 5 0 8）、販売機 3 0 0 0 が、カード 1 2 0 から転送されたキー K P m e d i a (1) を受信すると（ステップ S 5 1 0）、ディスプレイ 2 0 0 2 を介してユーザに料金投入を案内し、料金徴収を行なう（ステップ S 5 1 2）。続いて、販売機 3 0 0 0 は、セッションキー発生部 3 1 4 が、セッションキー K s を生成する。さらに、販売機 3 0 0 0 内の暗号化処理部 3 1 6 が、受信したキー K P

media (1) により、このセッションキー Ks を暗号化してデータ [Ks] Kmedia (1) を生成する (ステップ S 5 1 4)。

【0 2 4 7】

続いて、販売機 3 0 0 0 は、データ [Ks] Kmedia (1) をデータバス BS 1 に与え、コネクタ 2 0 1 0 から出力する (ステップ S 4 1 6)。携帯電話機 1 0 1 は、このデータ [Ks] Kmedia (1) を受信すると、メモリカード 1 2 0 に転送する (ステップ S 5 1 8)。

【0 2 4 8】

メモリカード 1 2 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス BS 3 に与えられた受信データ [Ks] Kmedia (1) を、復号処理部 1 4 0 4 が、キーデータ Kmedia (1) により復号処理することにより、セッションキーデータ Ks を復号し抽出する (ステップ S 5 2 0)。

【0 2 4 9】

続いて、暗号化処理部 1 4 0 6 は、KPcard (1) 保持部 1 4 0 5 から与えられる公開暗号化鍵 KPcard (1) および Ks 1 発生部 1 4 3 2 からのセッションキー Ks 1 を、セッションキー Ks により暗号化し (ステップ S 5 2 2)、データ [KPcard (1)、Ks 1] Ks を生成する (ステップ S 5 2 4)。

【0 2 5 0】

携帯電話機 1 0 1 は、暗号化処理部 1 4 0 6 により暗号化されたデータ [KPcard (1)、Ks 1] Ks を販売機 3 0 0 0 に対して送信する (ステップ S 5 2 6)。

【0 2 5 1】

販売機 3 0 0 0 では、コネクタ 2 0 1 0 を介してデータ [KPcard (1)、Ks 1] Ks が受信され (ステップ S 5 2 8)、データバス BS 1 に与えられたデータ [KPcard (1)、Ks 1] Ks を復号処理部 3 1 8 が、セッションキー Ks により復号処理して、キーデータ KPcard (1) およびキー Ks 1 を復号抽出する (ステップ S 5 3 0)。

【0 2 5 2】

続いて、配信制御部 3 1 2 は、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ等を含むライセンス情報データ L i c e n s e を生成する（ステップ S 5 3 2）。

【 0 2 5 3 】

さらに、販売機 3 0 0 0 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、コネクタ 2 0 1 0 を介して、携帯電話機 1 0 1 に送信する（ステップ S 5 3 4）。

【 0 2 5 4 】

携帯電話機 1 0 1 がデータ [D c] K c を受信すると（ステップ S 5 3 6）、メモリカード 1 2 0 においては、受信したデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する（ステップ S 5 3 8）。

【 0 2 5 5 】

一方、販売機 3 0 0 0 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し（ステップ S 5 4 0）、暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのキーデータ K c とライセンス情報データ L i c e n s e とを、復号処理部 3 1 8 より与えられたキーデータ K P c a r d (1) により暗号化処理する（ステップ S 5 4 2）。

【 0 2 5 6 】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [K c 、 L i c e n s e] K c a r d (1) を受取って、さらにセッションキー K s 1 により暗号化したデータをデータバス B S 1 に与え、暗号化処理部 3 2 2 により暗号化されたデータ [[K c , L i c e n s e] K c a r d (1)] K s 1 が携帯電話 1 0 1 に対して出力される（ステップ S 5 4 6）。

【 0 2 5 7 】

携帯電話 1 0 1 がデータ [[K c , L i c e n s e] K c a r d (1)] K s 1 を受信すると（ステップ S 5 4 8）、カード 1 2 0 においては、復号処理部 1 4 1 0 がセッションキー K s 1 により復号処理を行ない、データ [K c , L i c e n s e] K c a r d (1) を抽出し、メモリ 1 4 1 2 に格納する（ステップ S 5 5 2）。

【 0 2 5 8 】

以下の処理は、図 2 2 および図 2 3 に示した実施の形態 3 の処理と同様であるので、その説明は繰り返さない。

【 0 2 5 9 】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等の配信を受けることができる。

【 0 2 6 0 】

しかも、データバス上で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上するという効果がある。

【 0 2 6 1 】**[実施の形態 4 の変形例]**

実施の形態 4 のデータ配信システムにおいては、メモリカード 1 2 0 は、携帯電話 1 0 1 を介して、コンテンツデータ販売機 3 0 0 0 から暗号化コンテンツデータの配信を受ける構成であった。

【 0 2 6 2 】

しかしながら、図 2 7 に示した販売機 3 0 0 0 の構成において、実施の形態 3 の変形例と同様に、コネクタ 2 0 1 0 の代わりに、メモリカード 1 2 0 との間のインターフェースのためにメモリスロットを設ける構成とすれば、携帯電話 1 0 1 を介することなく、メモリカード 1 2 0 と販売機 3 0 0 0 とが直接データの授受を行うことが可能である。

【 0 2 6 3 】

このような実施の形態 4 の変形例のコンテンツデータ販売機 3 0 0 1 の構成は、データ処理部 2 1 0 0 の構成を除いて、図 2 4 に示した実施の形態 3 の変形例の構成と同様である。

【 0 2 6 4 】

すなわち、実施の形態 4 の変形例のコンテンツデータ販売機 3 0 0 1 の構成は、図 2 7 に示した実施の形態 4 の販売機 3 0 0 0 の構成と異なり、外部コネクタ 2 0 1 0 の代わりに、メモリカードを挿入できるカードスロット 2 0 3 0 が設け

られ、このカードスロット 2 0 3 0 がインターフェース部 2 0 1 2 を介して、データバス B S 1 とデータの授受をする構成となっている。

【0 2 6 5】

図 3 0 および図 3 1 は、実施の形態 4 の変形例のデータ配信システムにおける配信動作を説明するための第 1 および第 2 のフローチャートである。

【0 2 6 6】

図 2 8 および図 2 9 に示した実施の形態 3 の配信動作とは、携帯電話 1 0 1 を介さずに、メモリカード 1 2 0 と販売機 3 0 0 1 がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

【0 2 6 7】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

【0 2 6 8】

しかも、メモリカードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、音楽データの再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

【0 2 6 9】

なお、以上説明してきた各実施の形態において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作権情報や音楽サーバ 3 0 に対するアクセス情報等を、付加情報 D i として暗号化コンテンツデータと併せて配信することも可能である。この付加データ D i は、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されて音楽データとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ 1 4 1 2 に記録される。

【0 2 7 0】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範

囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0 2 7 1】

【発明の効果】

以上説明したとおり、本願発明にかかる配信システムでは、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となり、かつ、1度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

【0 2 7 2】

また、ユーザが配信キャリアを介してではなく、販売機により暗号化コンテンツデータを購入することができるので、ユーザの利便性が一層向上する。

【図面の簡単な説明】

【図 1】 本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【図 2】 図 1 に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

【図 3】 図 1 に示した音楽サーバ 3 0 の構成を示す概略ブロック図である。

【図 4】 図 1 に示した携帯電話 1 0 0 の構成を説明するための概略ブロック図である。

【図 5】 図 4 に示したメモリカード 1 1 0 の構成を説明するための概略ブロック図である。

【図 6】 図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信動作を説明するための第 1 のフローチャートである。

【図 7】 図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信動作を説明するための第 2 のフローチャートである。

【図 8】 携帯電話 1 0 0 内において音楽情報を復号化し、音楽として外部

に出力するための再生処理を説明するフローチャートである。

【図 9】 2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第1のフローチャートである。

【図 10】 2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第2のフローチャートである。

【図 11】 実施の形態2のメモリカード120に対応した音楽サーバ31の構成を示す概略ブロック図である。

【図 12】 実施の形態2における携帯電話機101の構成を説明するための概略ブロック図である。

【図 13】 本発明の実施の形態2のメモリカード120の構成を説明するための概略ブロック図である。

【図 14】 図13で説明したメモリカード120を用いた配信動作を説明するための第1のフローチャートである。

【図 15】 図13で説明したメモリカード120を用いた配信動作を説明するための第2のフローチャートである。

【図 16】 携帯電話101内において音楽情報を復号化し、音楽として外部に出力するための再生処理を説明する第1のフローチャートである。

【図 17】 携帯電話101内において音楽情報を復号化し、音楽として外部に出力するための再生処理を説明する第2のフローチャートである。

【図 18】 2つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第1のフローチャートである。

【図 19】 2つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第2のフローチャートである。

【図 20】 実施の形態3のデータ配信システムの構成を説明するための概念図である。

【図 21】 実施の形態3のコンテンツデータ販売機2000の構成を示す概略ブロック図である。

【図 2 2】 図 2 0 および図 2 1 で説明したデータ配信システムにおける配信動作を説明するための第 1 のフローチャートである。

【図 2 3】 図 2 0 および図 2 1 で説明したデータ配信システムにおける配信動作を説明するための第 2 のフローチャートである。

【図 2 4】 実施の形態 3 の変形例のコンテンツデータ販売機 2 0 0 1 の構成を示す概念図である。

【図 2 5】 実施の形態 3 の変形例のデータ配信システムにおける配信動作を説明するための第 1 のフローチャートである。

【図 2 6】 実施の形態 3 の変形例のデータ配信システムにおける配信動作を説明するための第 2 のフローチャートである。

【図 2 7】 実施の形態 4 のコンテンツデータ販売機 3 0 0 0 の構成を説明するための概略ブロック図である。

【図 2 8】 図 2 7 で説明したデータ配信システムにおける配信動作を説明するための第 1 のフローチャートである。

【図 2 9】 図 2 7 で説明したデータ配信システムにおける配信動作を説明するための第 2 のフローチャートである。

【図 3 0】 実施の形態 4 の変形例のデータ配信システムにおける配信動作を説明するための第 1 のフローチャートである。

【図 3 1】 実施の形態 4 の変形例のデータ配信システムにおける配信動作を説明するための第 2 のフローチャートである。

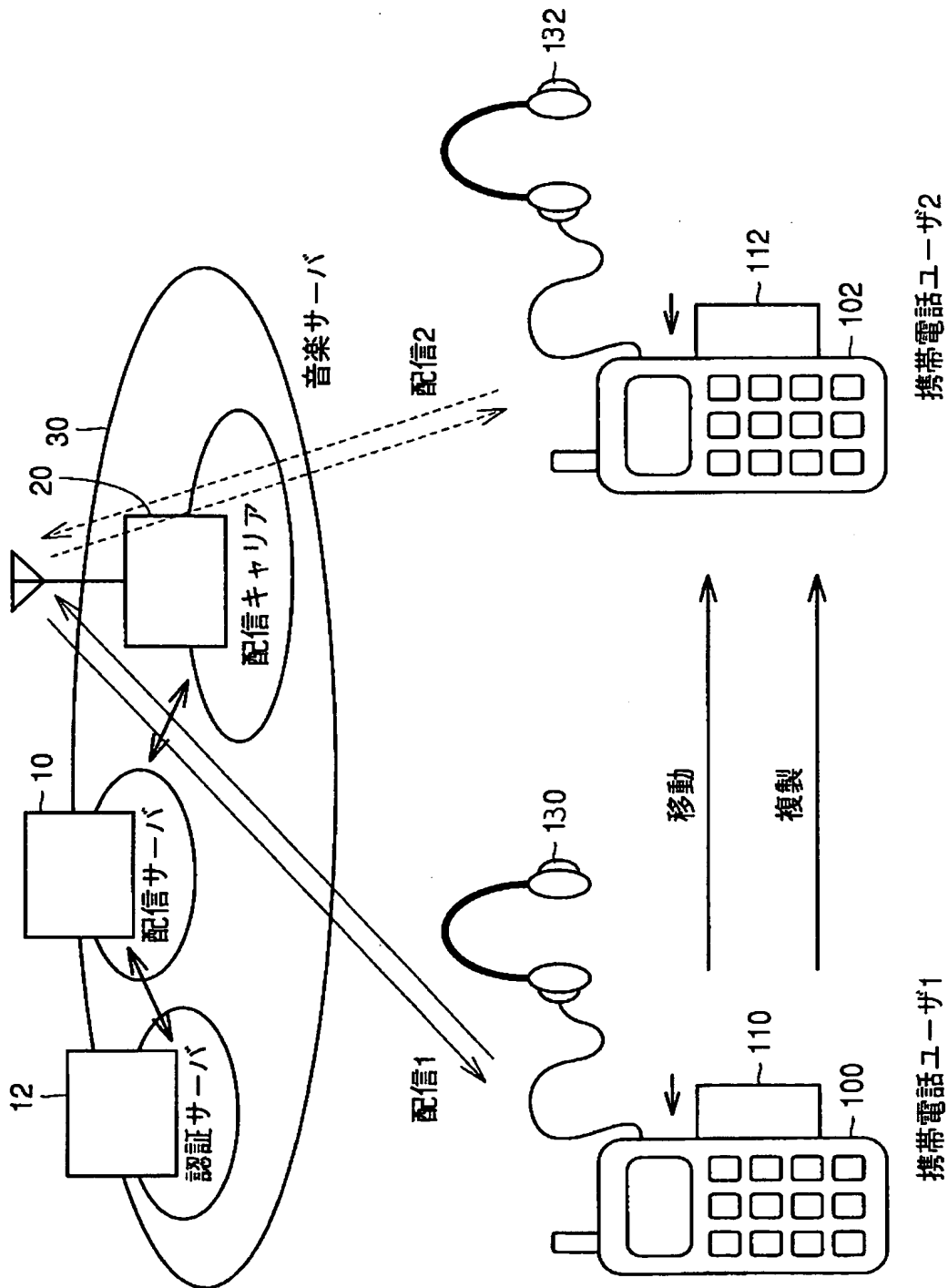
【符号の説明】

1 0 コンテンツサーバ、2 0 配信キャリア、3 0, 3 1 音楽サーバ、1 0 0, 1 0 1, 1 0 2, 1 0 3 携帯電話機、1 1 0, 1 1 2, 1 2 0, 1 2 2 メモリカード、1 3 0, 1 3 2 ヘッドホン、1 1 0 2 アンテナ、1 1 0 4 送受信機、1 1 0 6 コントローラ、1 1 0 8 タッチキー部、1 1 1 0 ディスプレイ、1 1 1 2 音声再生部、1 2 0 0 メモリインタフェース、1 4 0 4 復号処理部、1 4 0 6 暗号化処理部、1 4 0 8, 1 4 0 9 切替スイッチ、1 4 1 0 復号処理部、1 4 1 2 メモリ、1 4 1 4 暗号化処理部、1 4 1 6 復号処理部、1 4 2 0 コントローラ、1 4 3 0 暗号化処理部、1 4 3 2

セッションキー発生部、1 4 3 4, 1 4 3 5 切替スイッチ、1 5 0 2 セッションキー発生部、1 5 0 4 暗号化処理部、1 5 0 6 復号処理部、1 5 0 8 音楽再生部、1 5 1 0 混合部、1 5 1 2 デジタルアナログ変換器、2 0 0 , 3 0 0 0 コンテンツデータ販売機。

【書類名】 図面

【図 1】

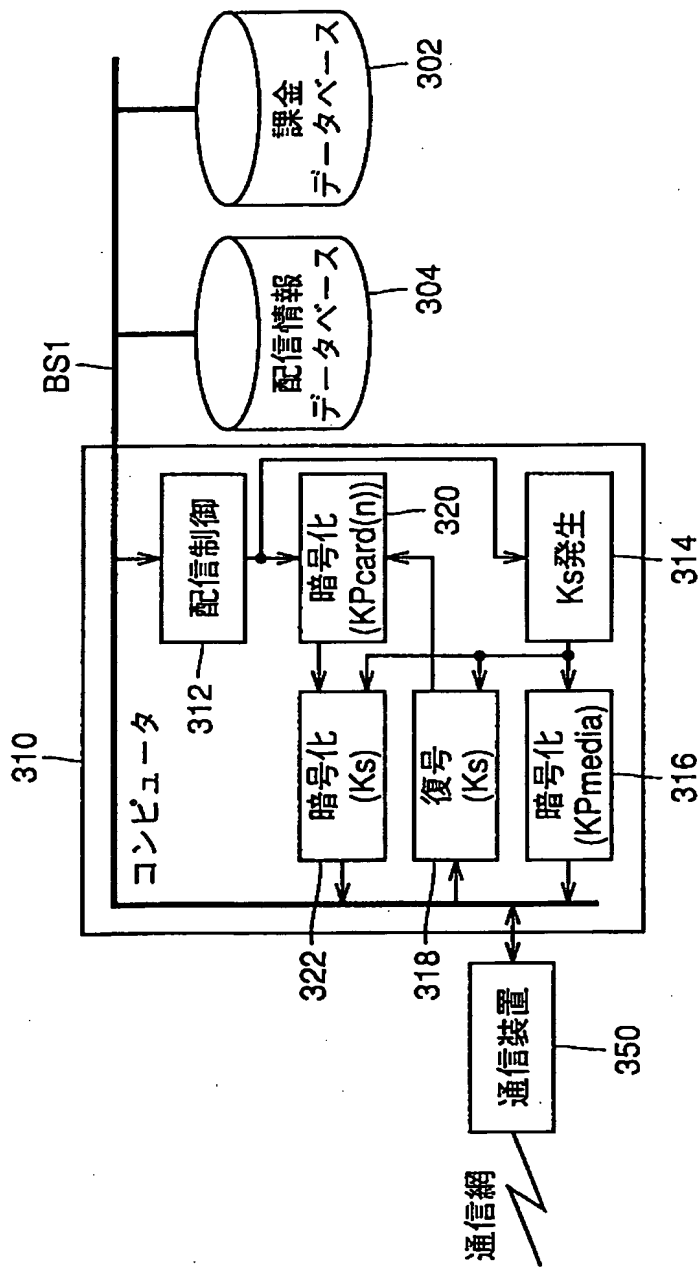


【図 2】

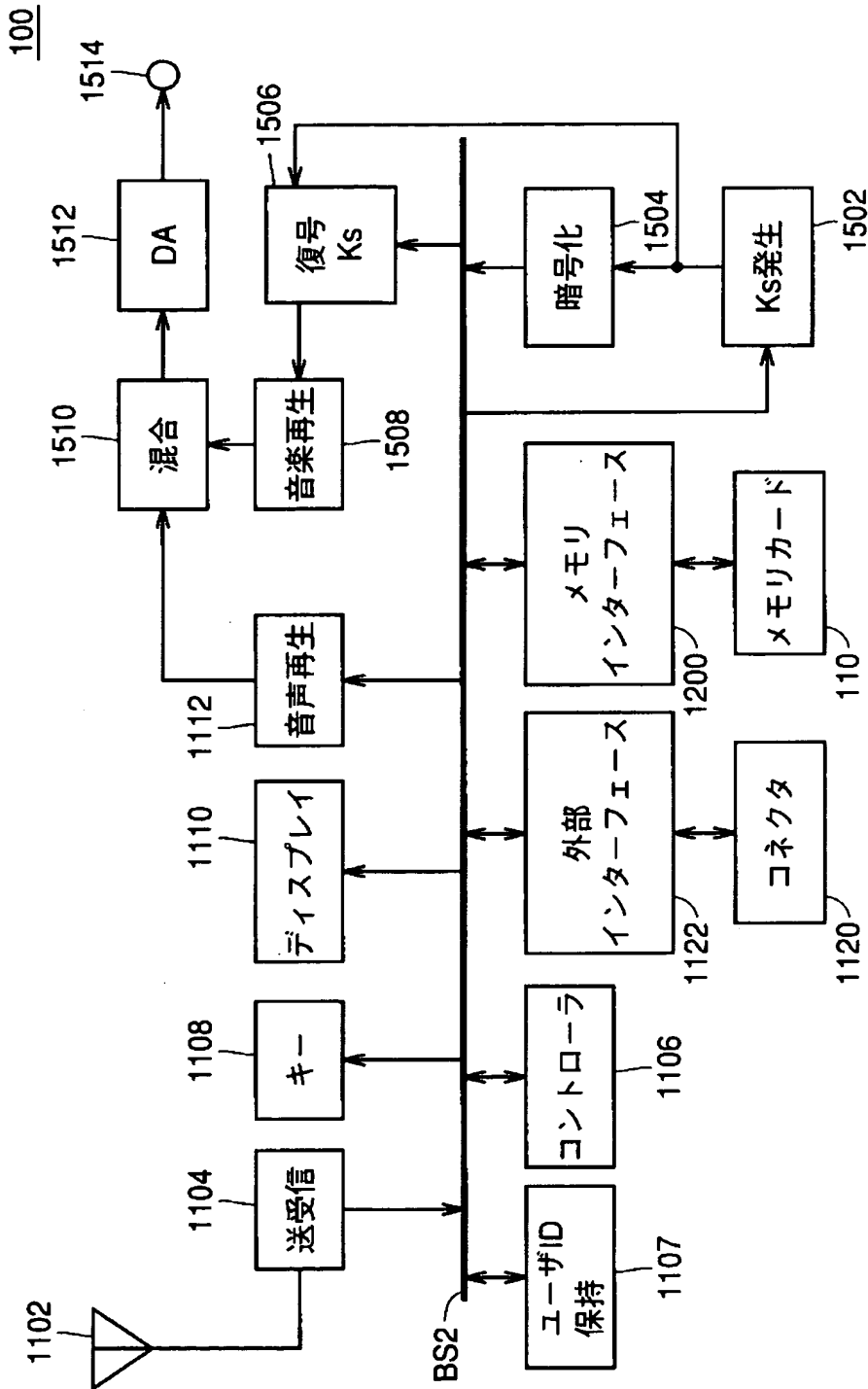
	記号	属性	特性	
			媒体固有	メモリカードの種類ごとに固有な情報を有する
メモリカード内 管理の鍵	Kmedia(n)	秘密復号鍵		メモリカード毎に異なる
	Kcard(n)	秘密復号鍵		
	KPcard(n)	公開暗号化鍵		Kcard(n)と対を成す。 KPcard(n)により暗号化されたデータは、Kcard(n)で復号可能
メモリカード外 管理の鍵	KPmedia(n)	公開暗号化鍵	媒体固有	Kmediaと対を成す。 KPmediaにより暗号化されたデータは、Kmediaで復号可能。
	Ks	共通鍵	セッション 固有	通信毎（例：アクセス毎）に発生。 配信サーバ、携帯電話機にて管理
配信データ	Kc	共通鍵	ライセンス キー	暗号化コンテンツデータの復号鍵
	License-ID	再生に関する 情報		例：曲目の特定情報 再生回数の制限情報
	User-ID	受信者を識別 する情報		例：電話番号
	Dc	コンテンツ データ		例：音楽情報データ
	[Dc]Kc	暗号化コン テンツデータ		共通鍵Kcにより暗号化されたコンテンツデータ

【図 3】

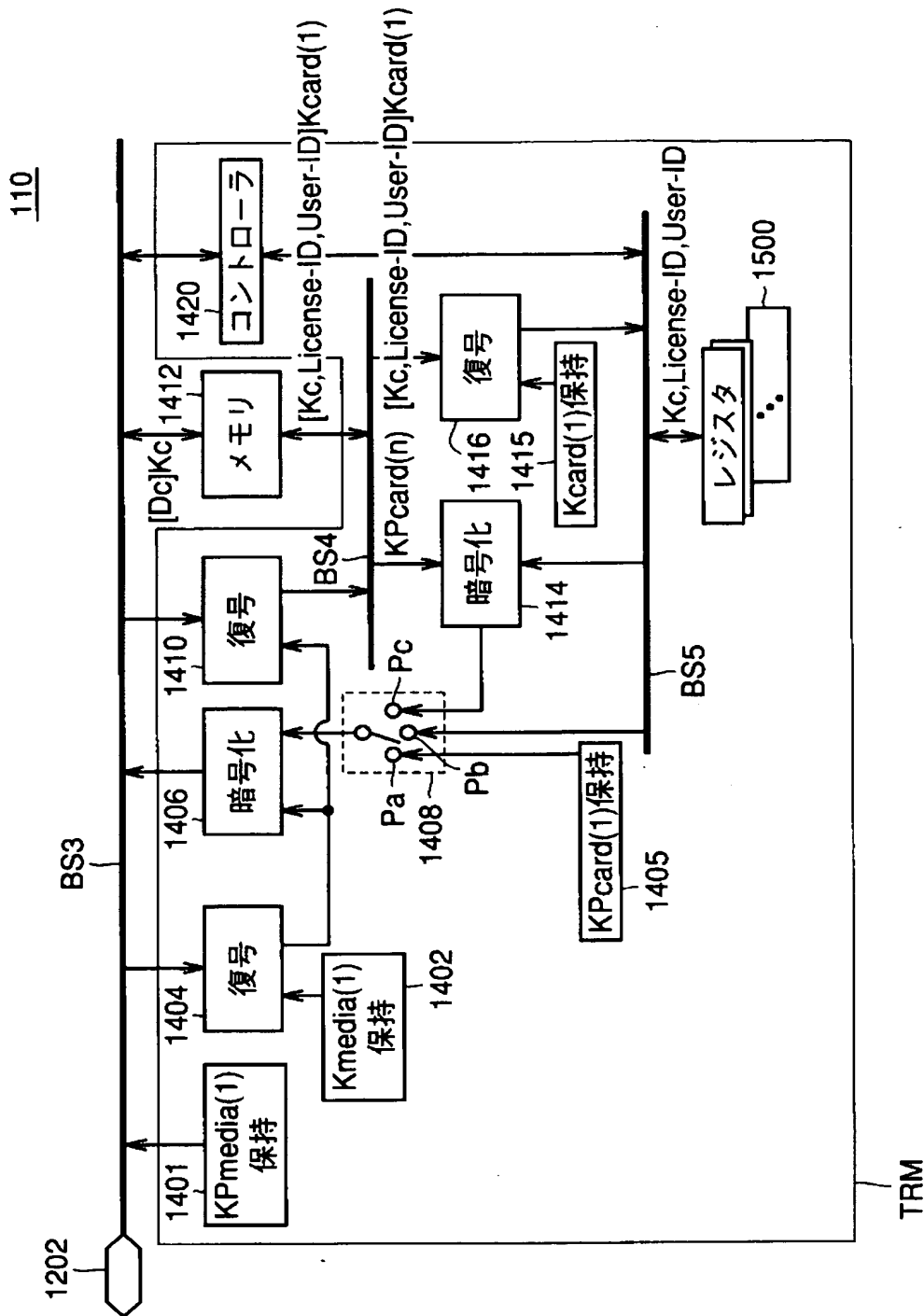
30



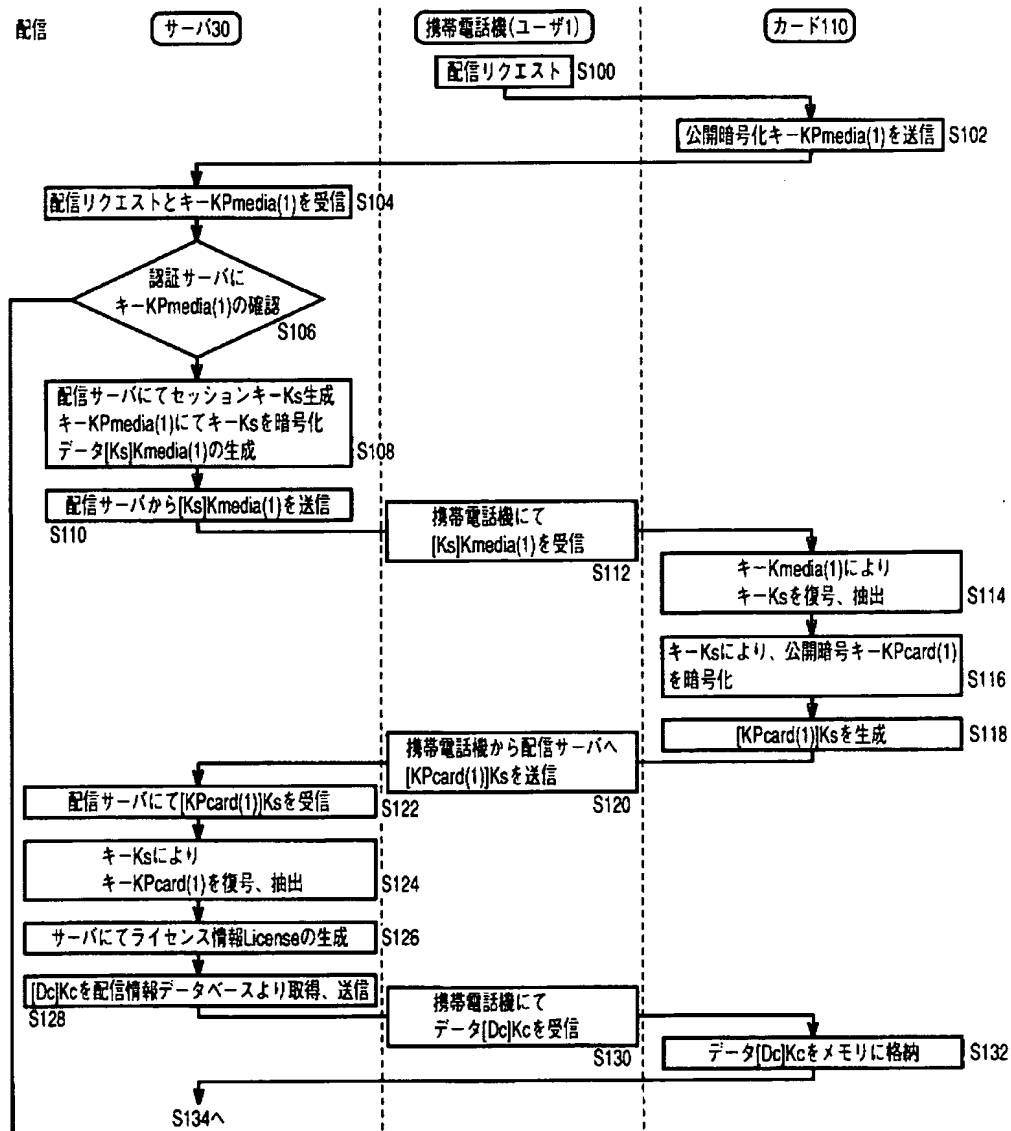
【図 4】



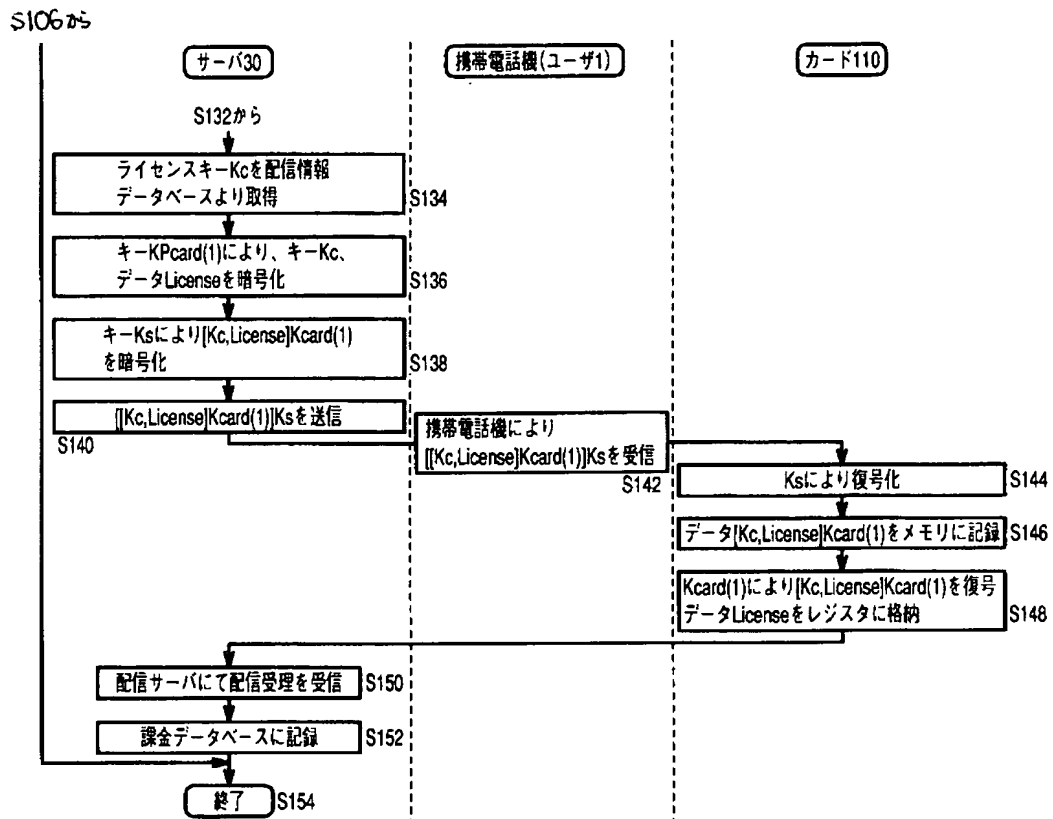
【図 5】



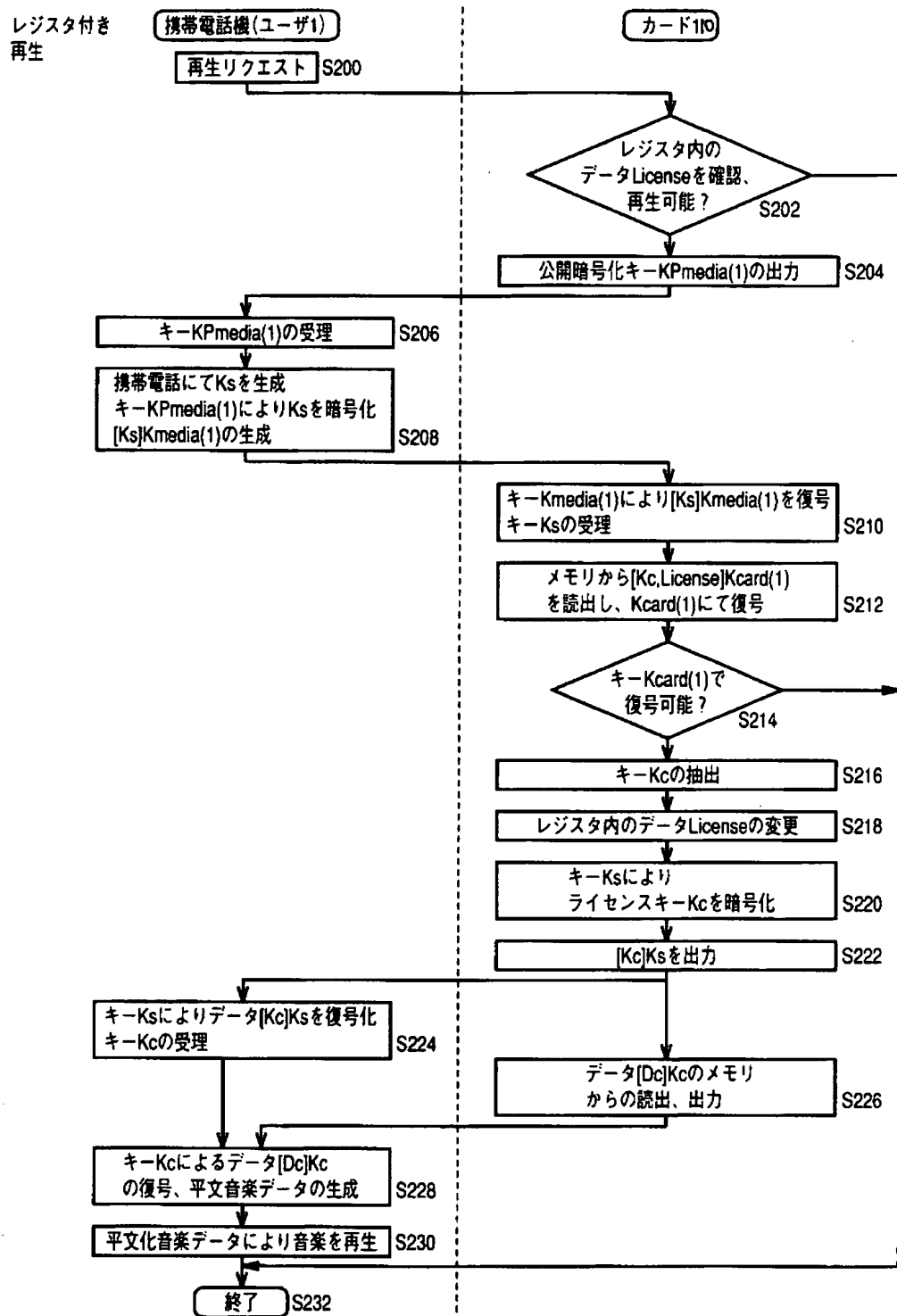
【図 6】



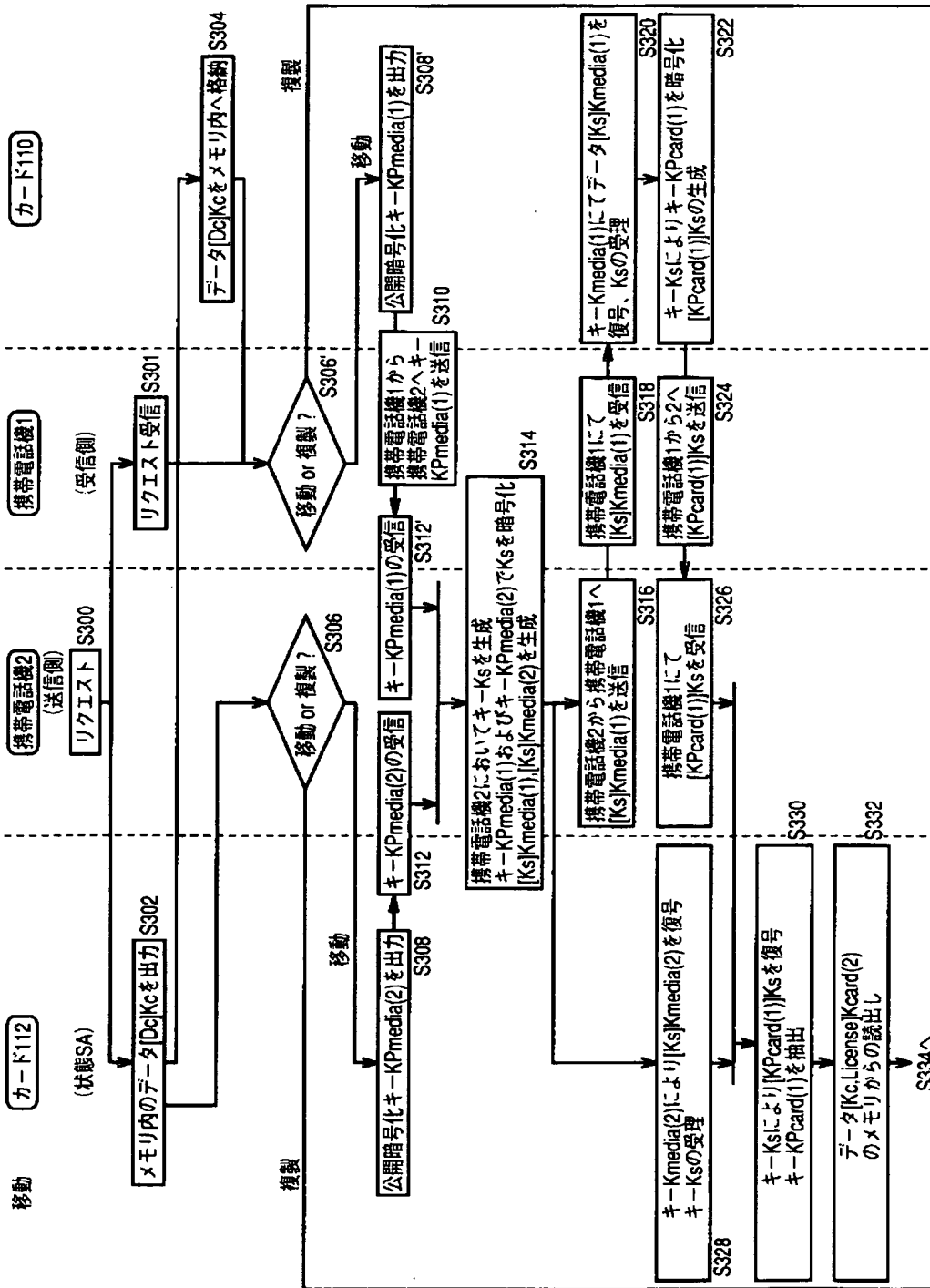
【図 7】



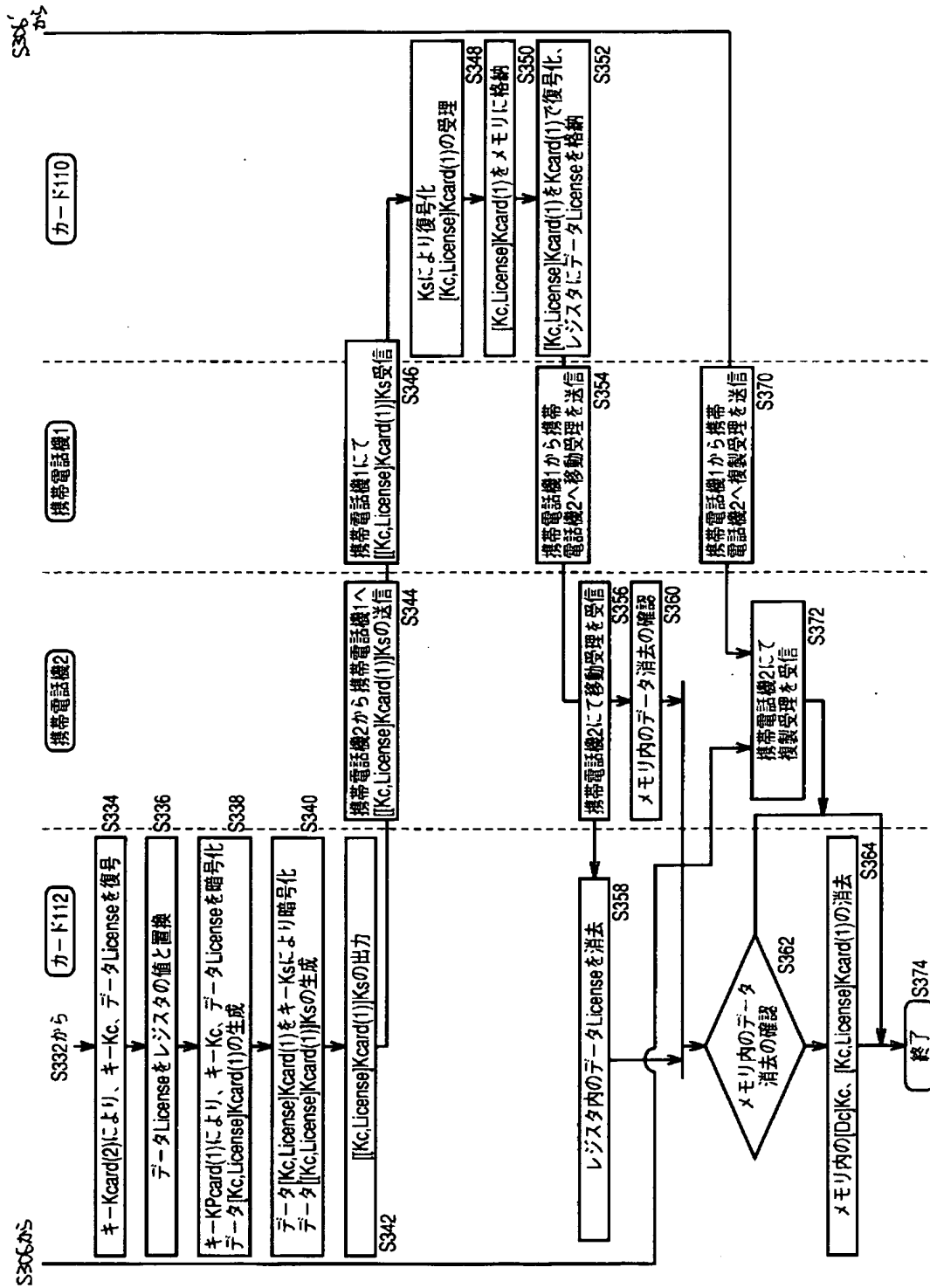
【図 8】



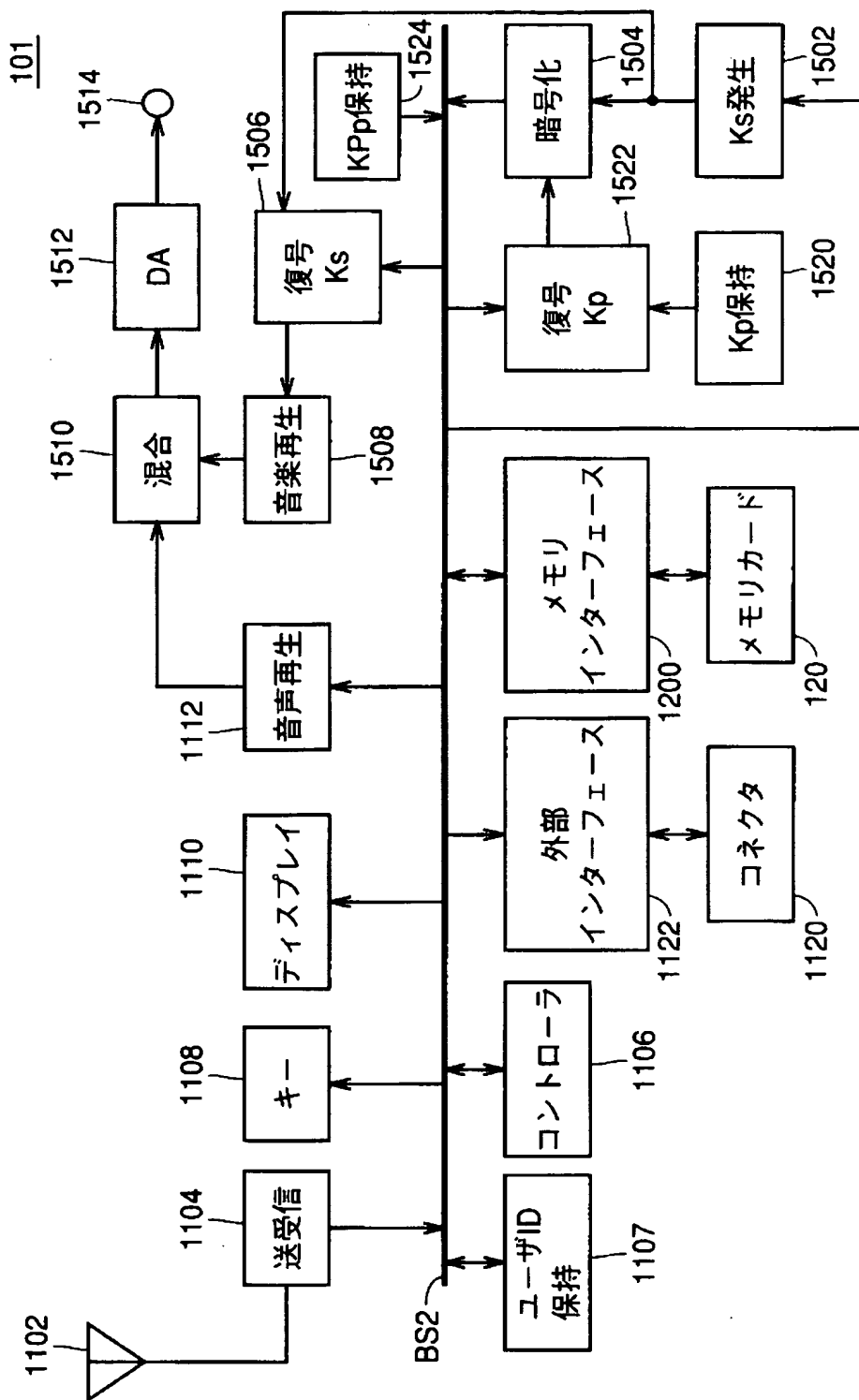
【図 9】



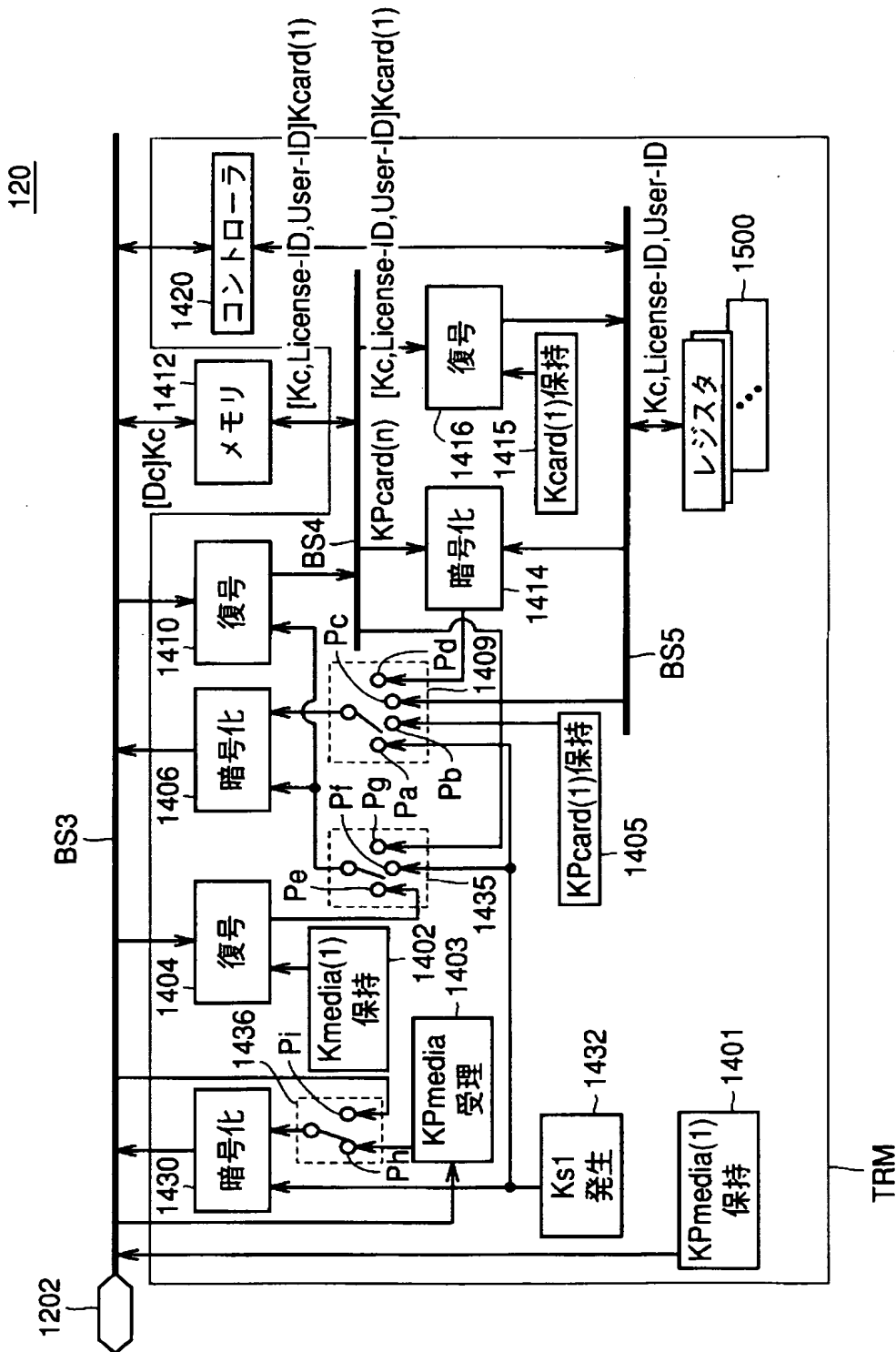
【図 10】



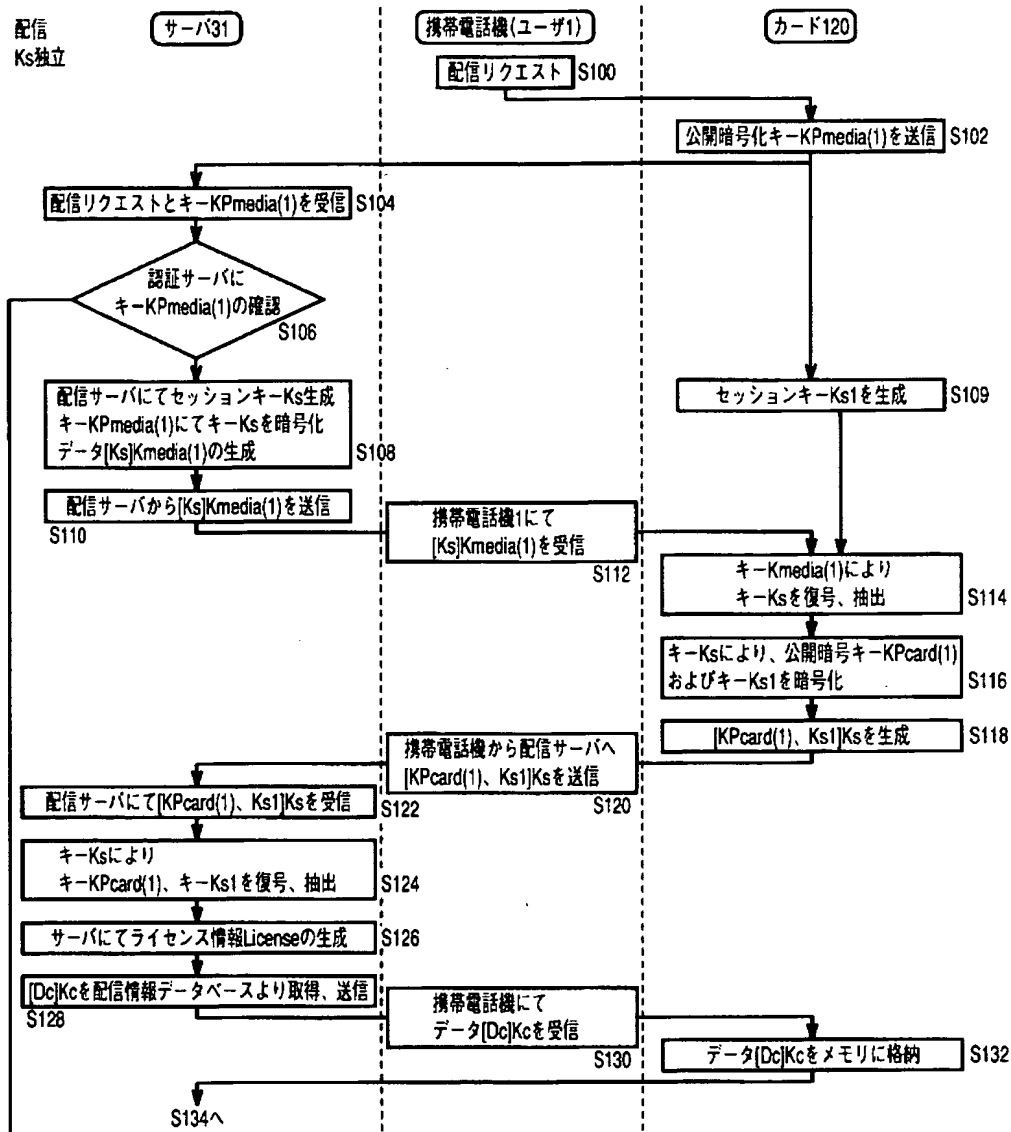
【図 1 2】



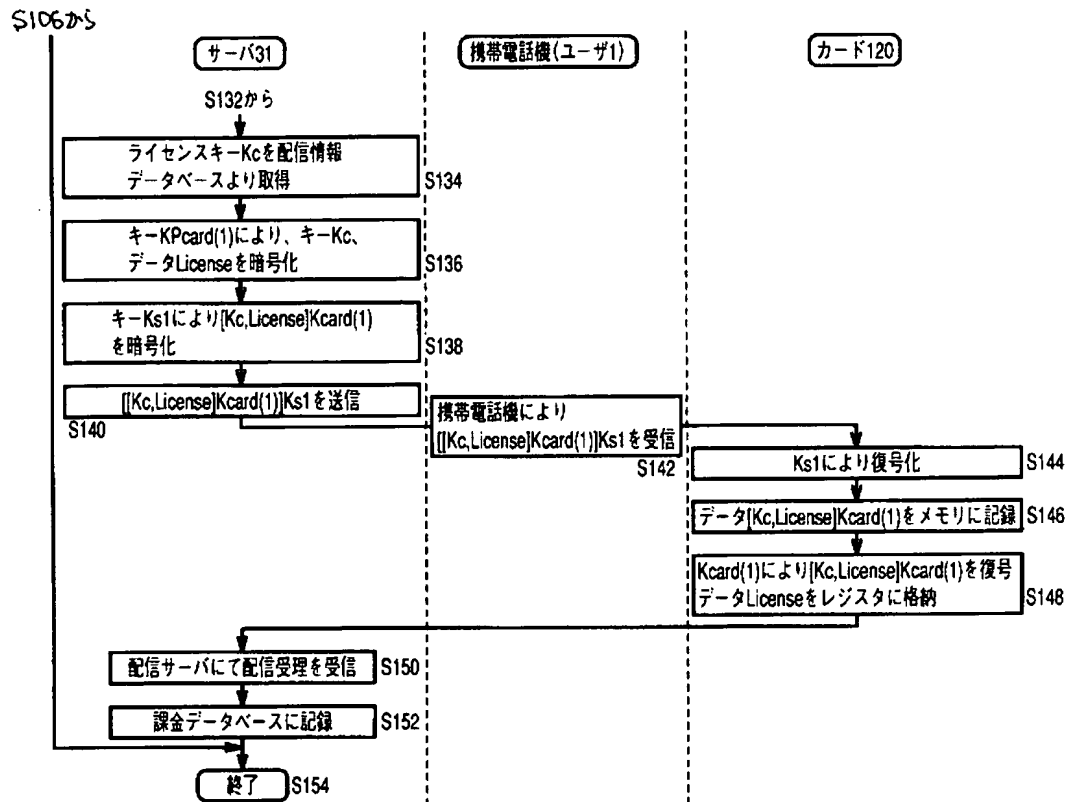
【図 1 3】



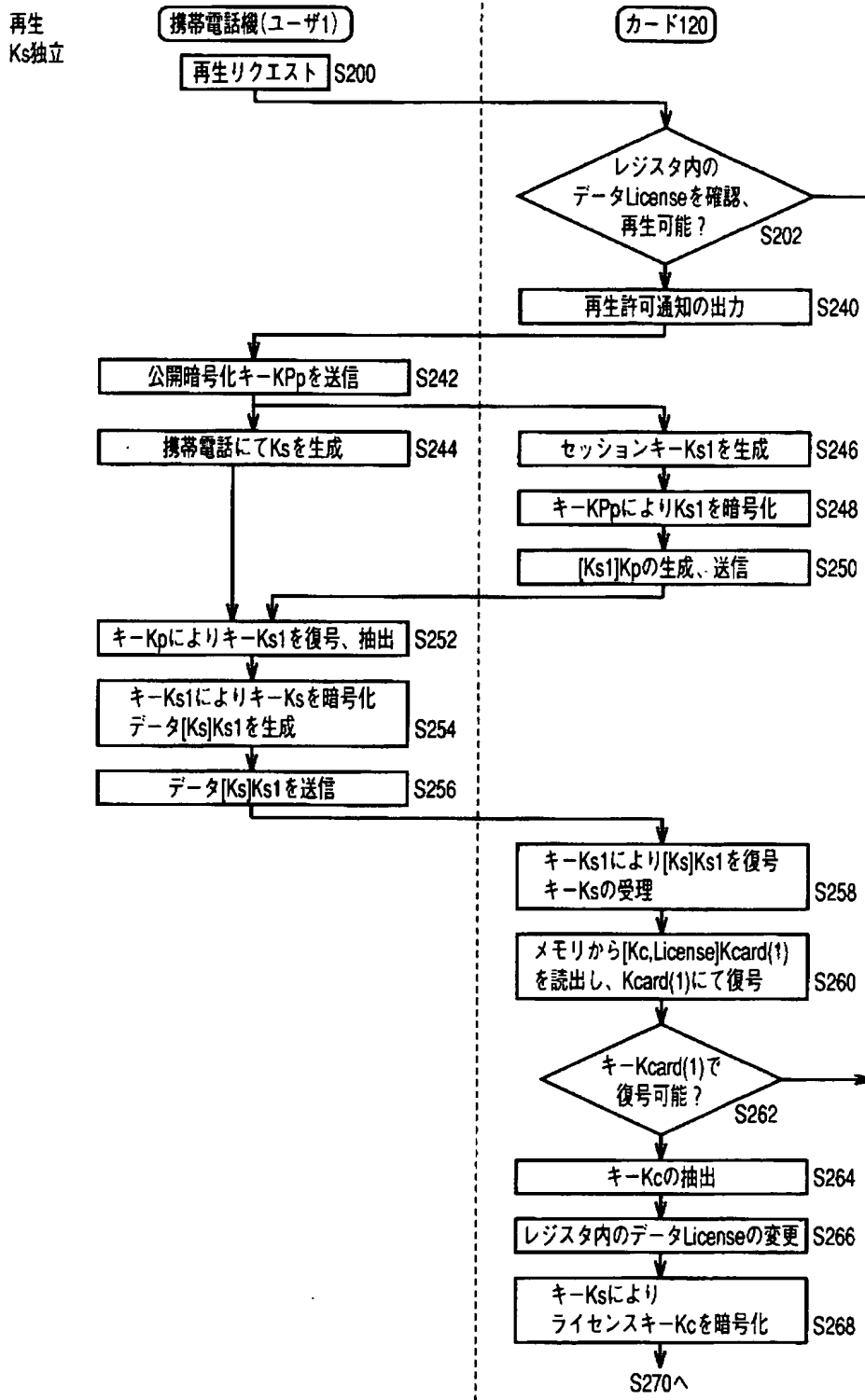
【図 1 4】



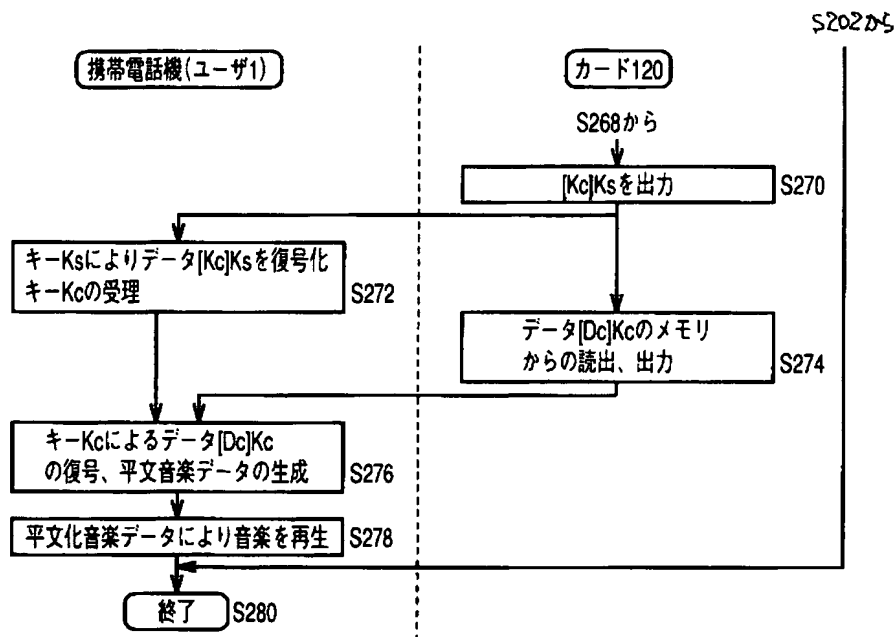
【図 1 5】



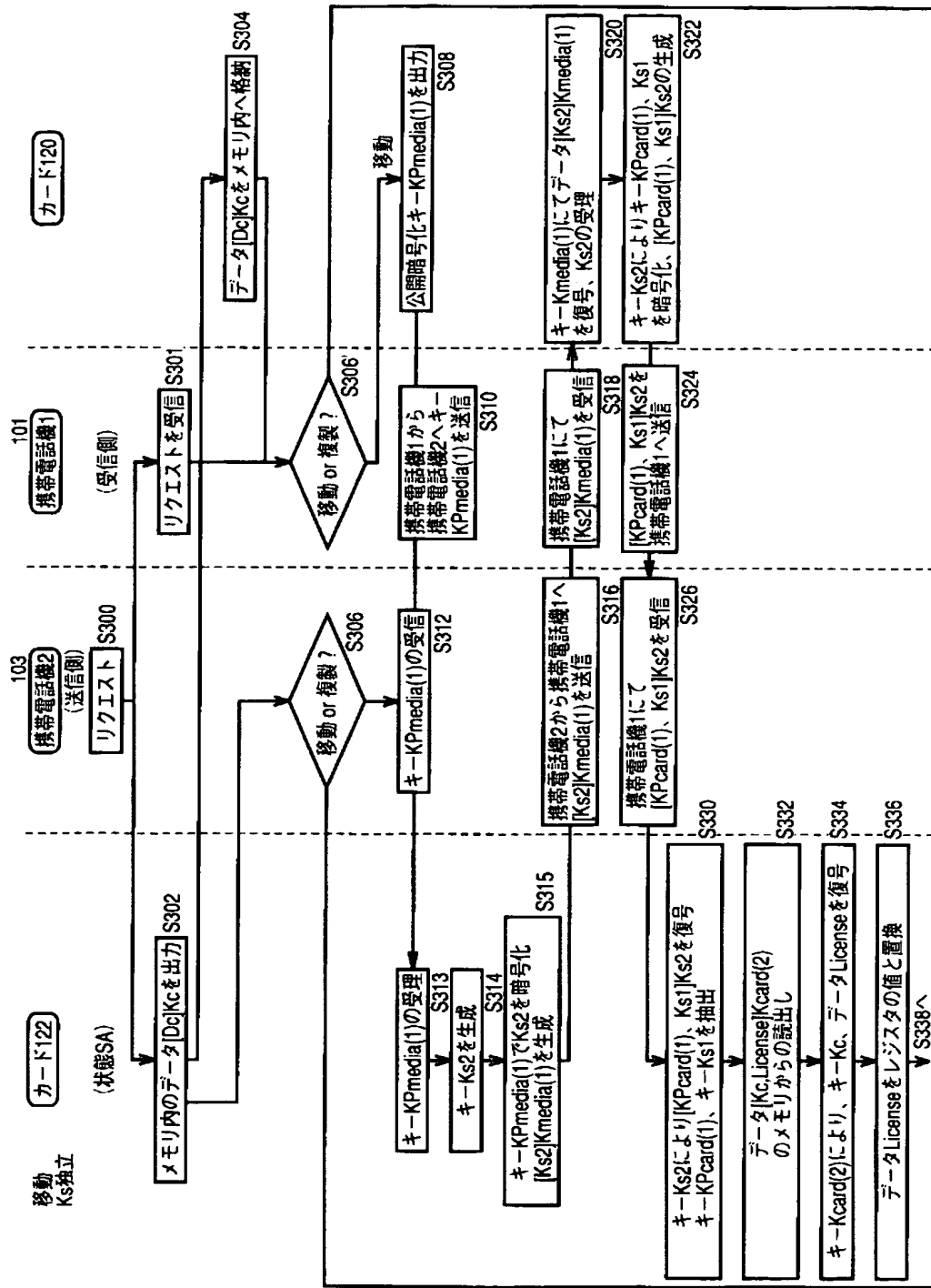
【図 1 6】



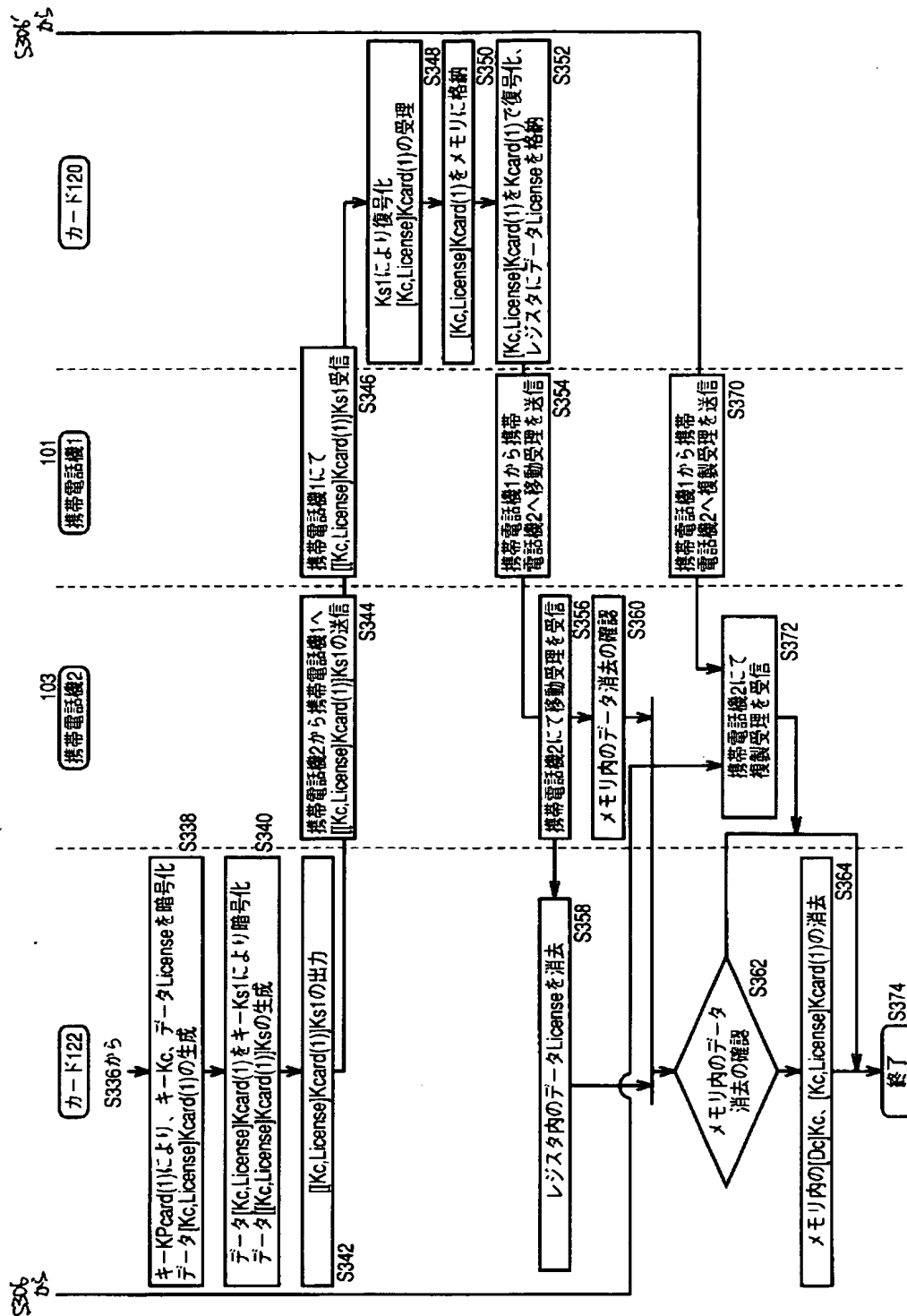
【図 1 7】



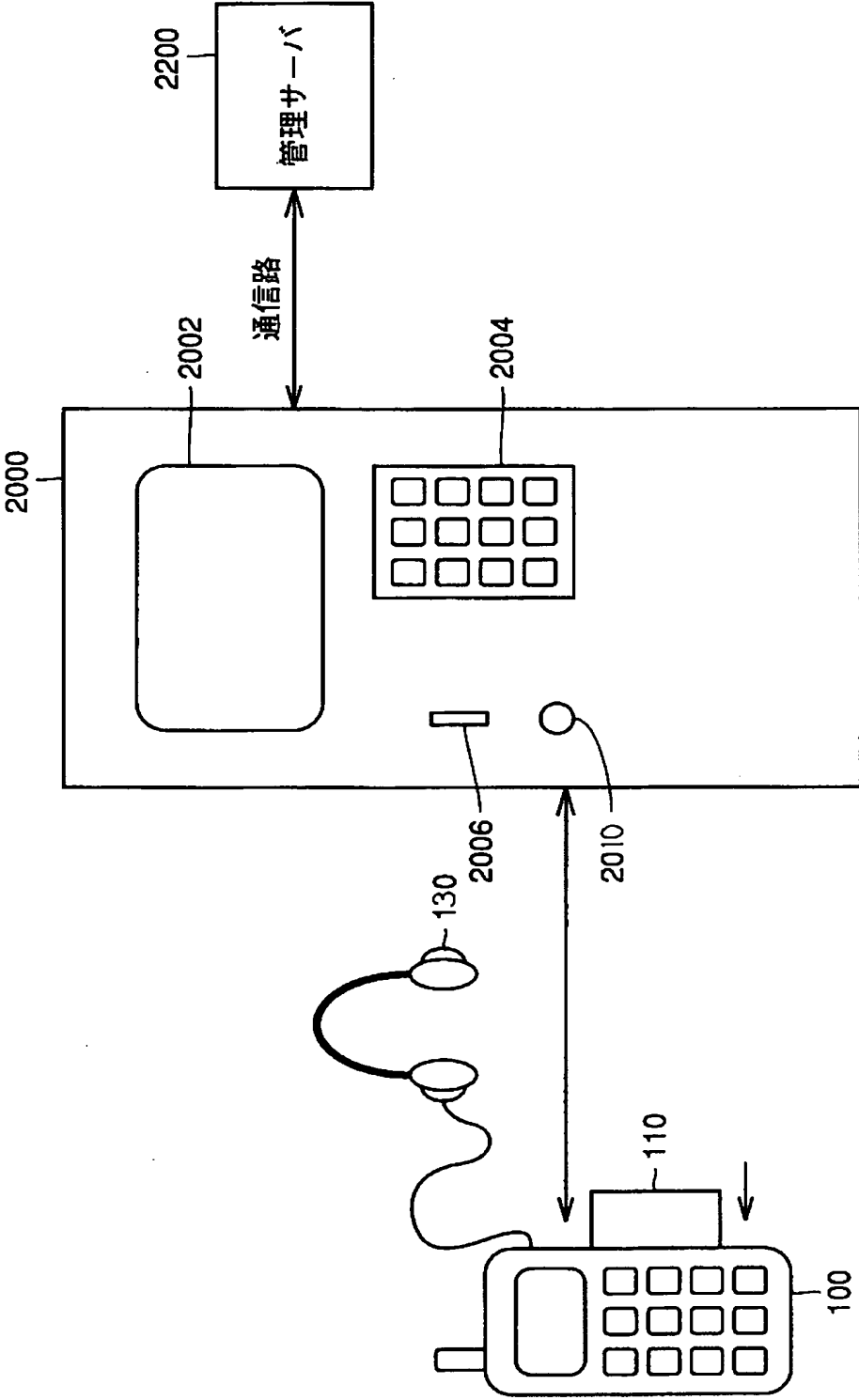
【図 1 8】



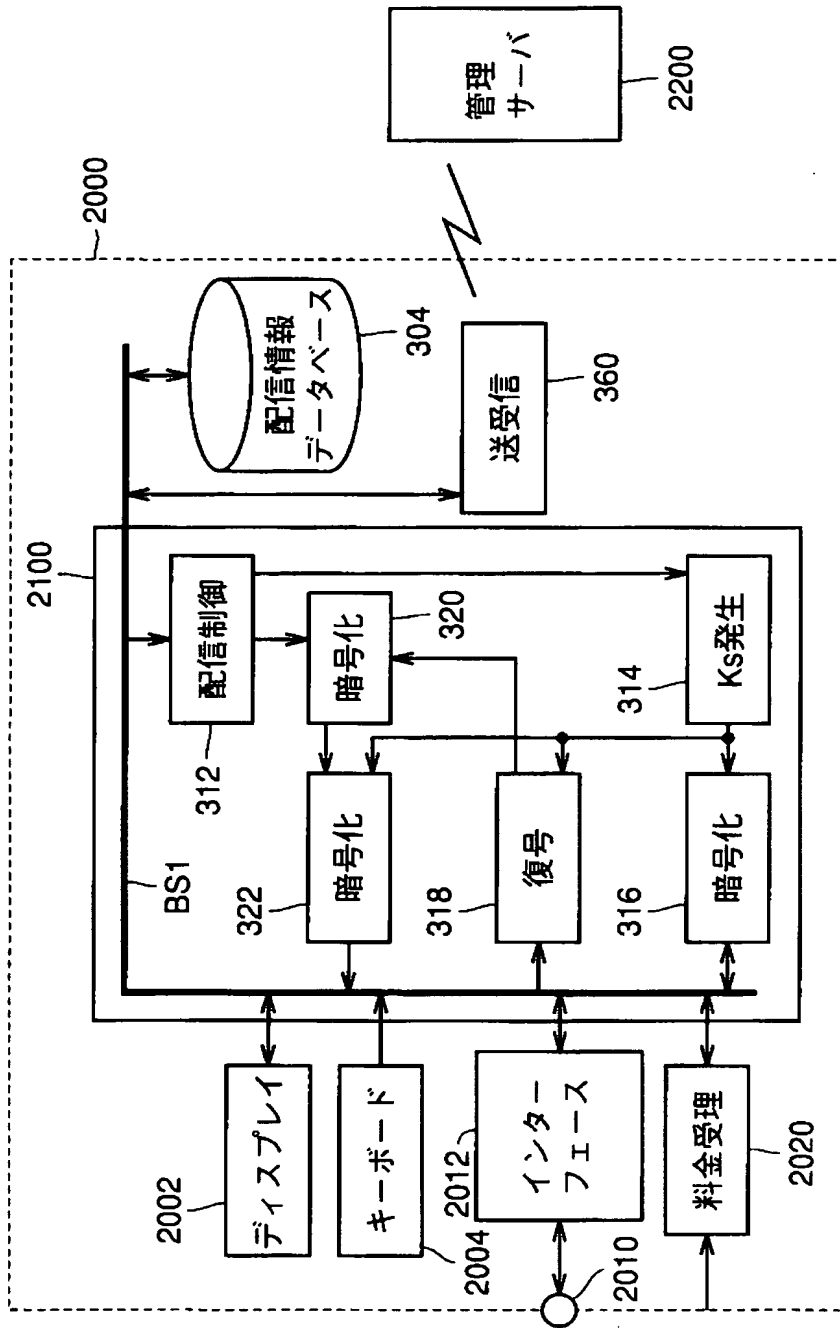
【図 1 9】



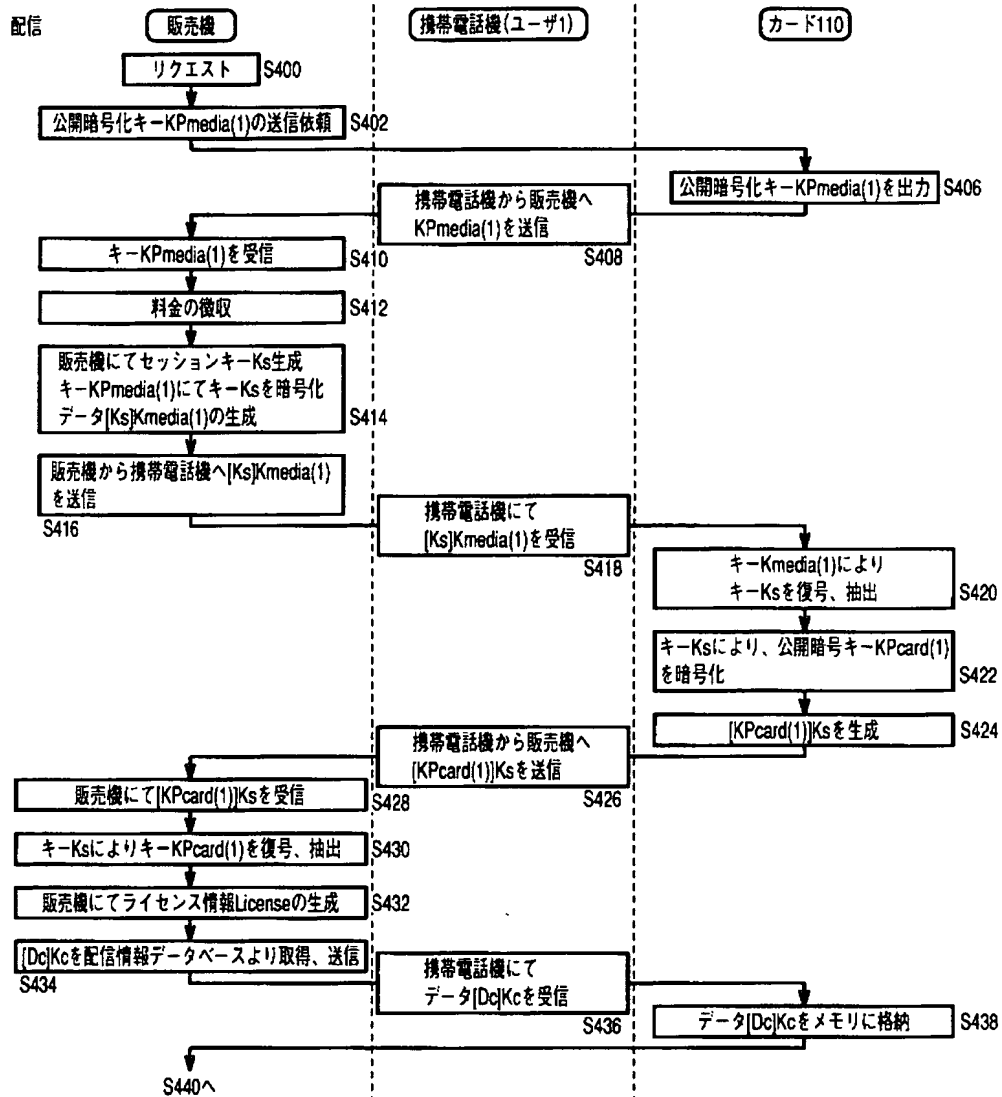
【図 2 0】



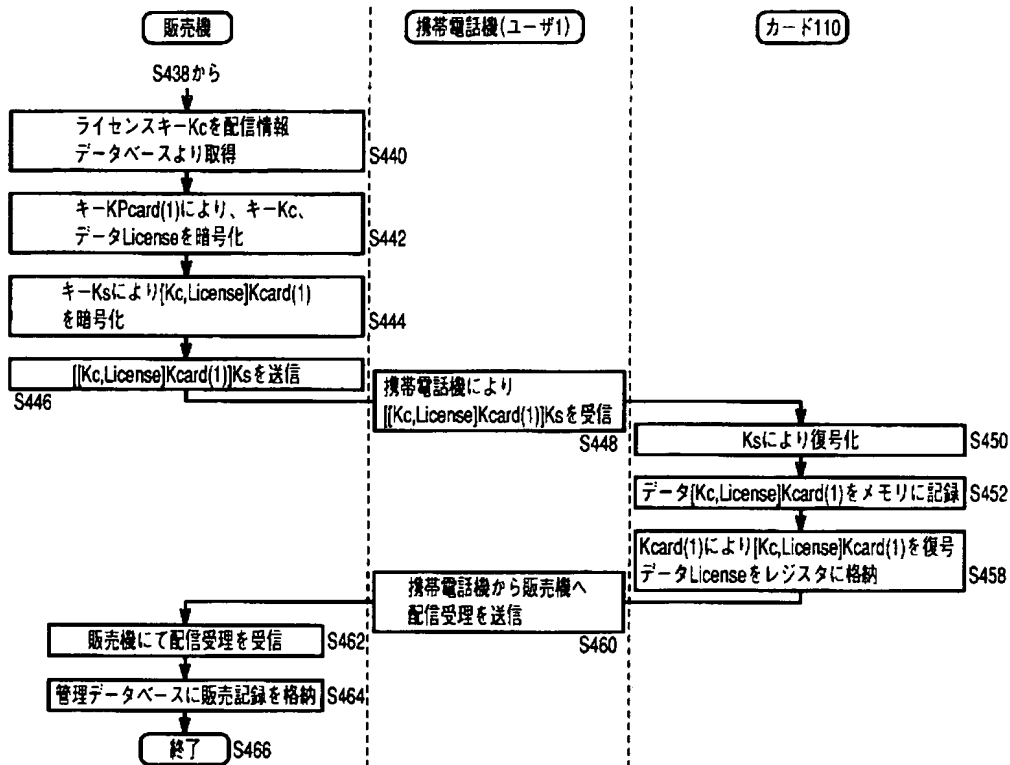
【図 2 1】



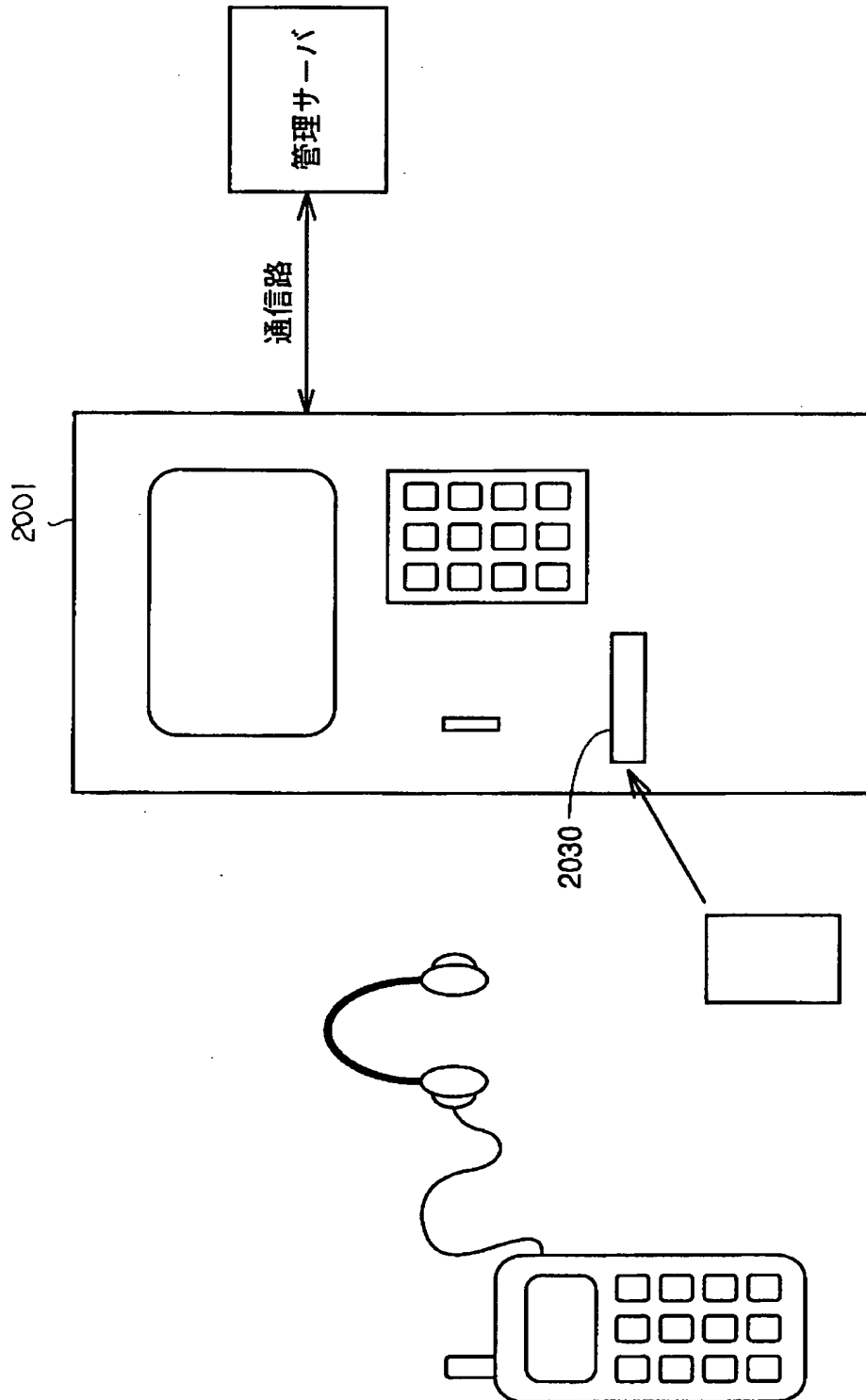
【図 2 2】



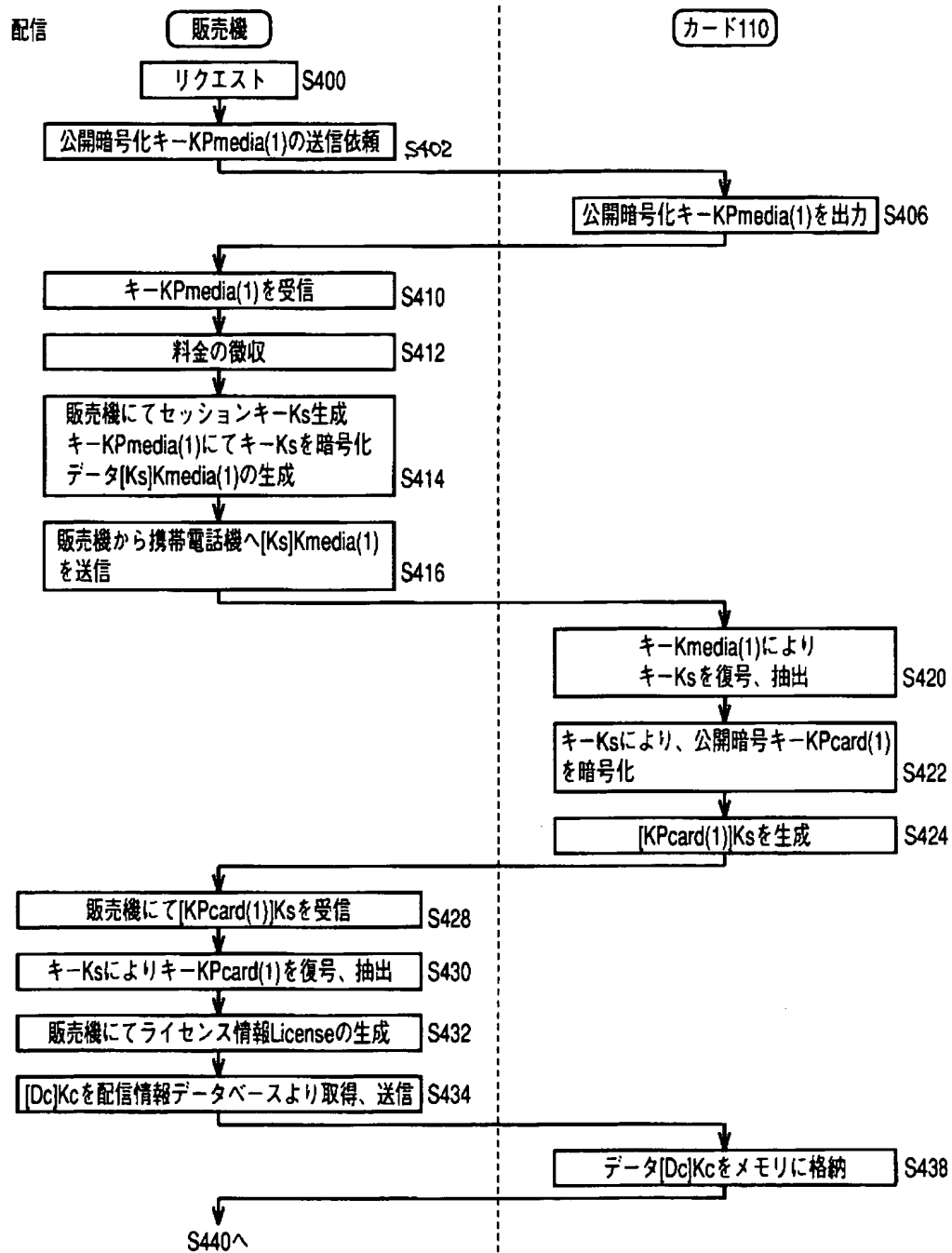
【図 2 3】



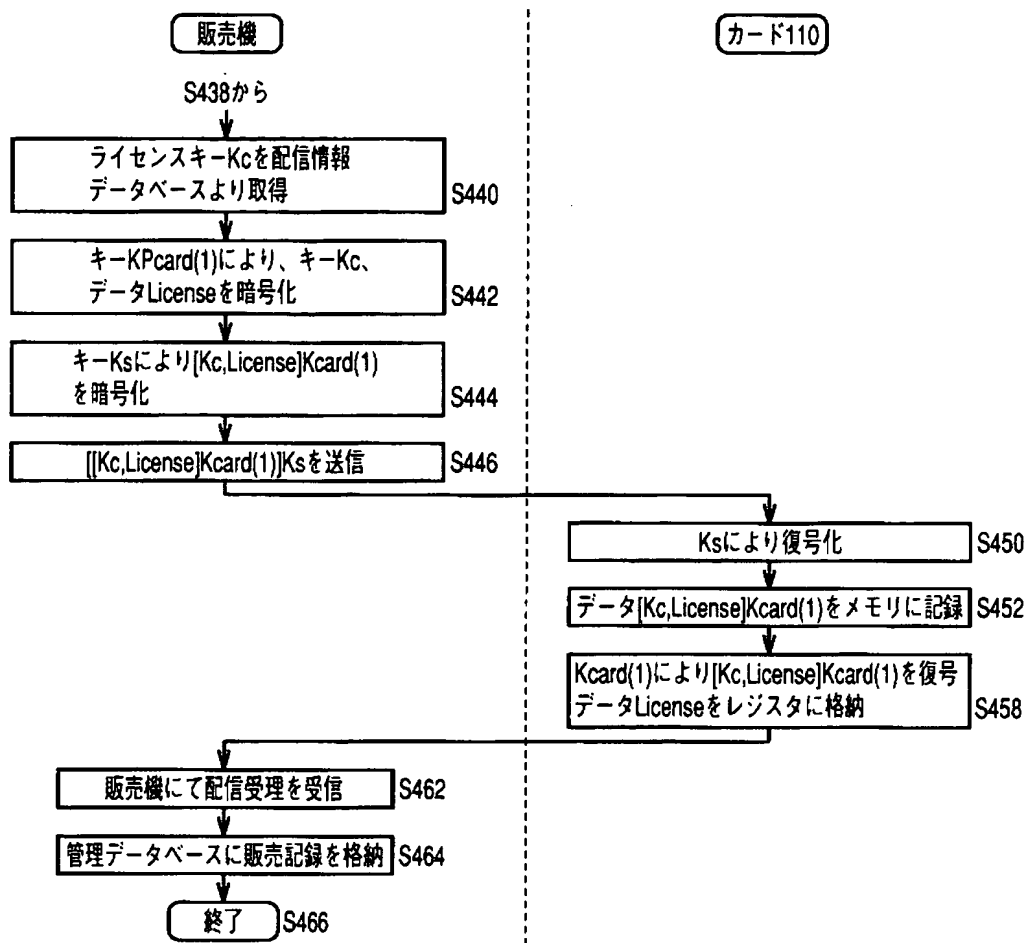
【図 2 4】



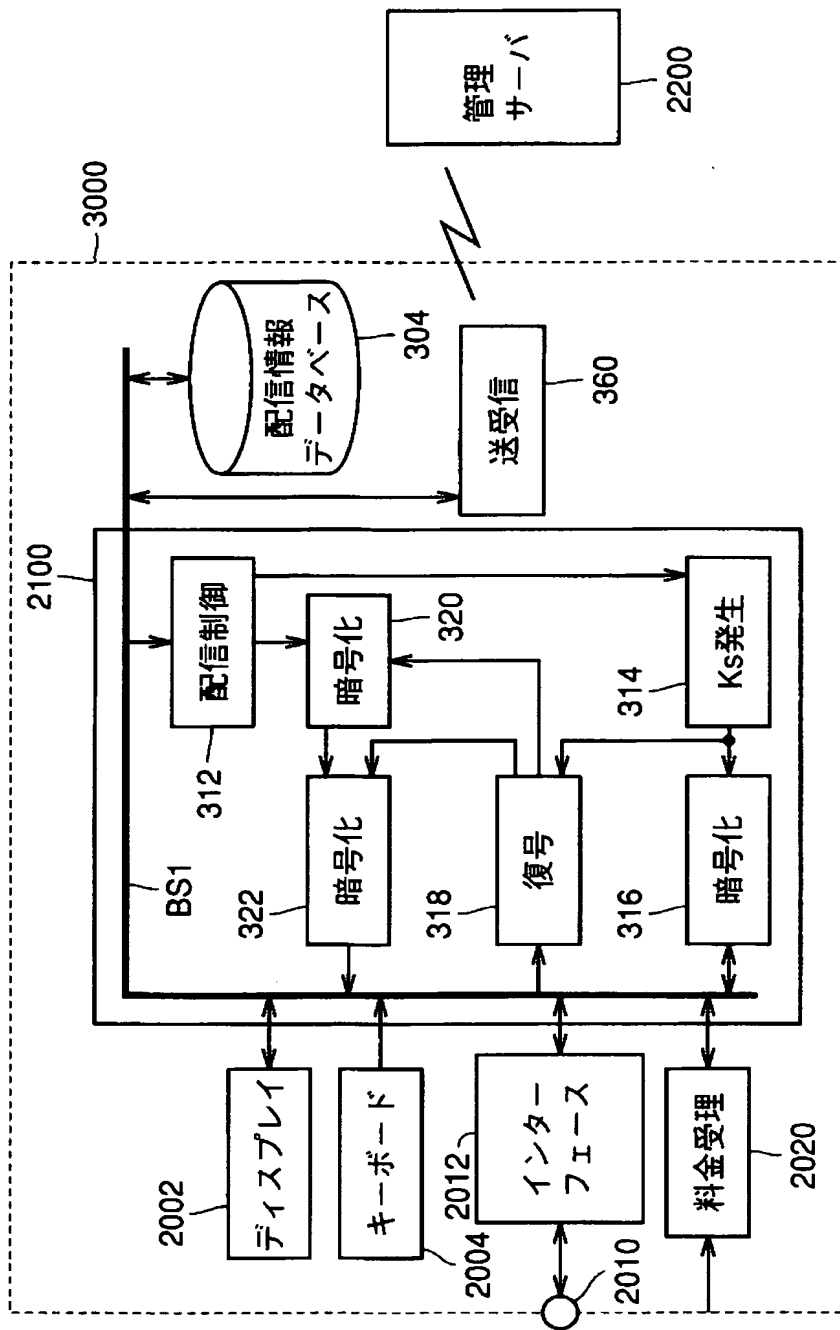
【図 2 5】



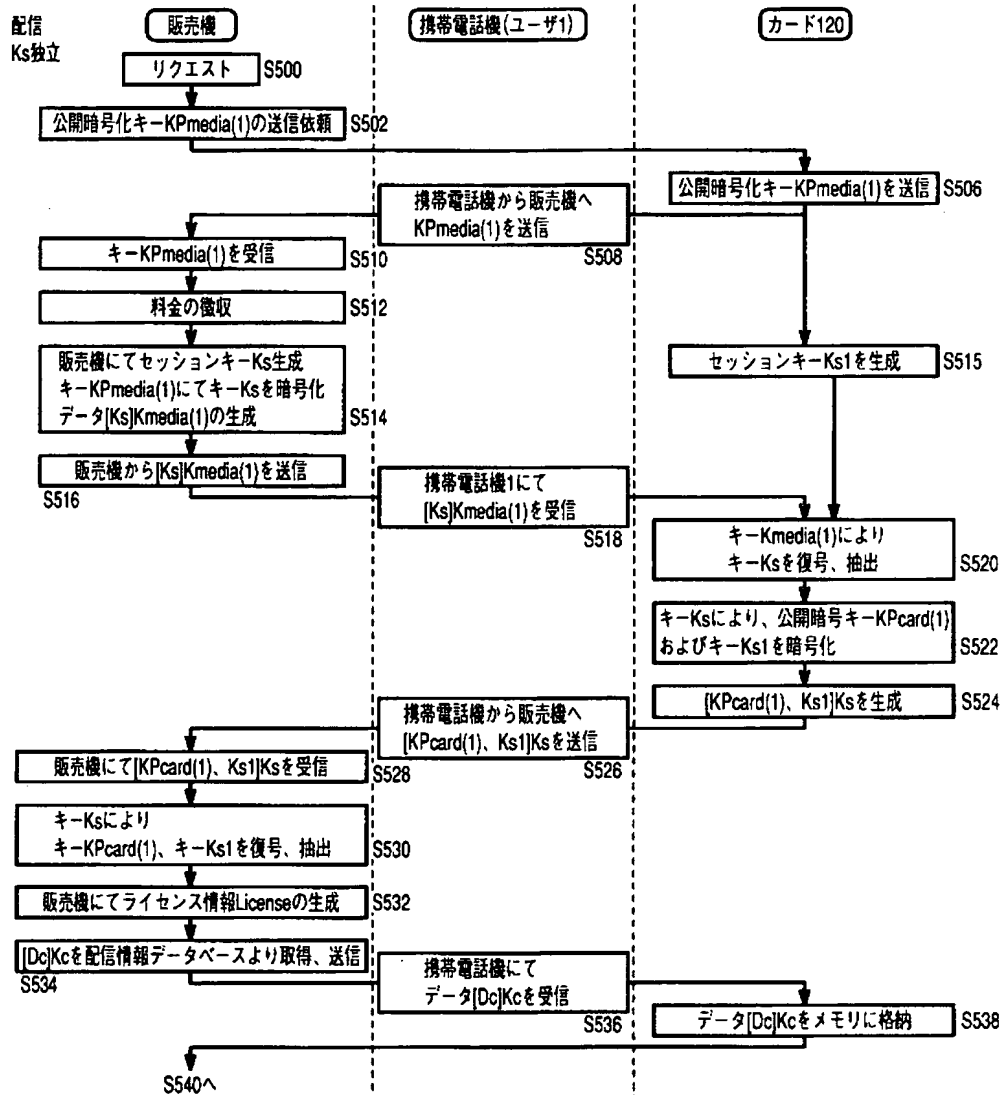
【図 2 6】



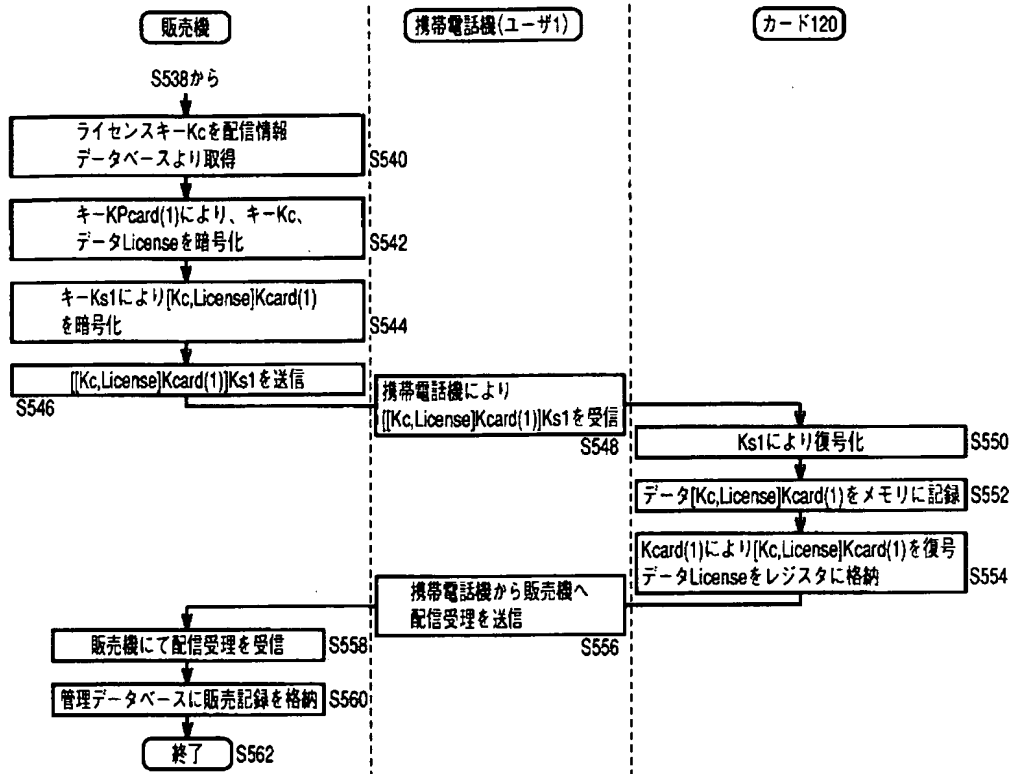
【図 2 7】



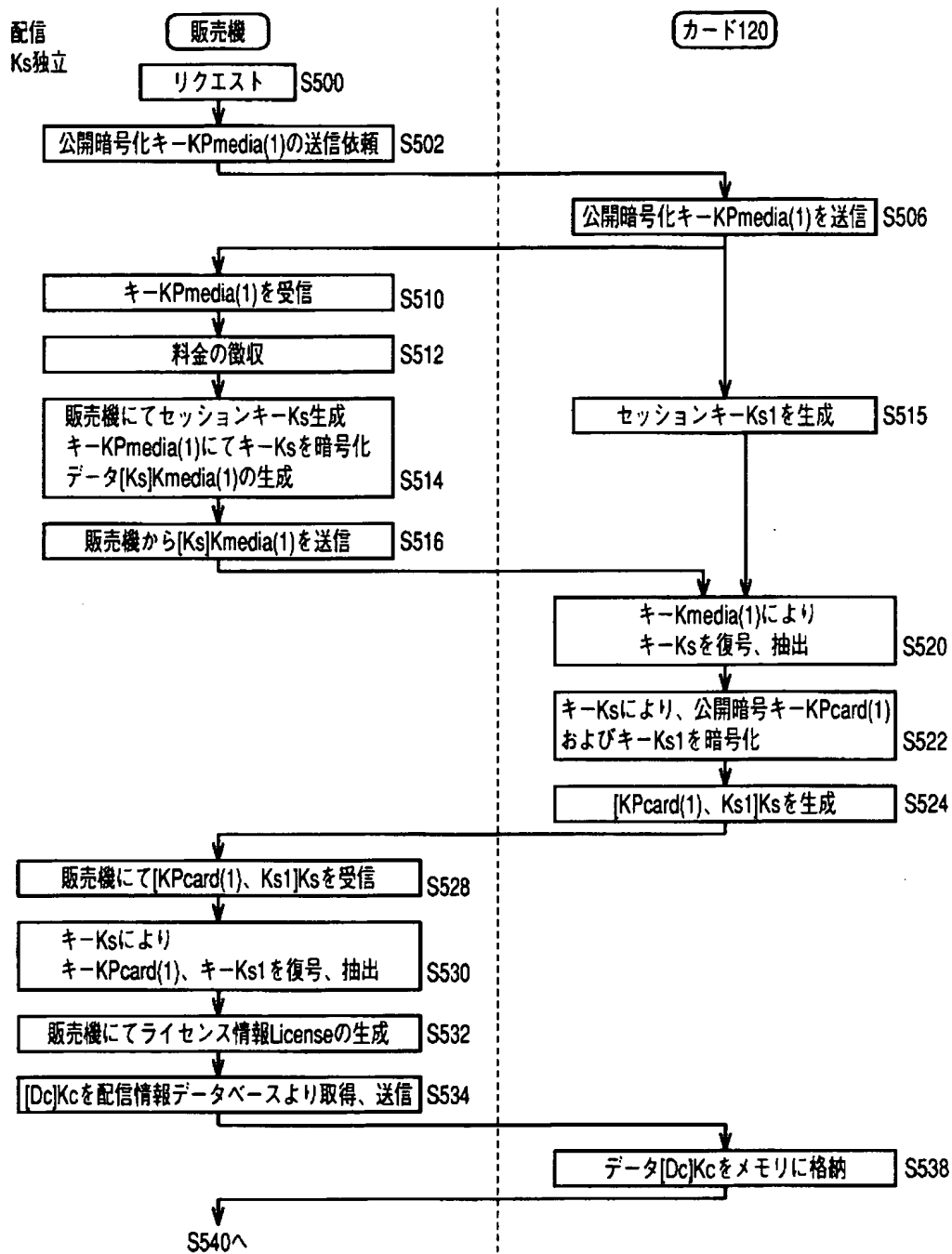
【図 2 8】



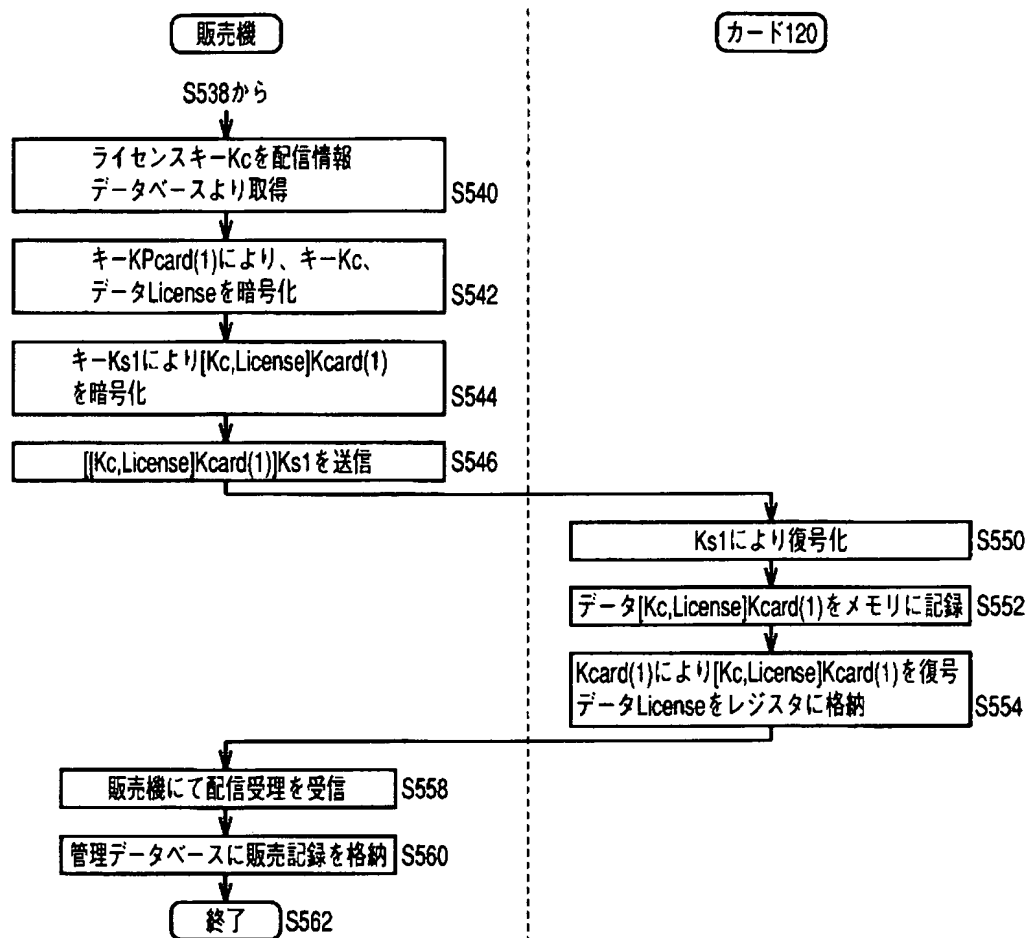
【図 2 9】



【図 3 0】



【図 3 1】



【書類名】 要約書

【要約】

【課題】 著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供する。

【解決手段】 メモリカード 1 1 0 は、サーバから携帯電話網を介してデータベース B S 3 に与えられるデータから、復号処理をすることによりセッションキー K s を抽出する。暗号化処理部 1 4 0 6 は、セッションキー K s に基づいて、メモリカード 1 1 0 の公開暗号化鍵 K P c a r d (1) を暗号化してデータベース B S 3 を介してサーバに与える。レジスタ 1 5 0 0 は、復号されたライセンス I D、ユーザ I D 等のデータをサーバから受けとって格納し、メモリ 1 4 1 2 は、データベース B S 3 からライセンスキー K c により暗号化されている暗号化コンテンツデータ [D c] K c を受けて格納する。

【選択図】 図 5

認定・付加情報

特許出願の番号	平成 1 1 年 特許願 第 2 4 1 7 4 7 号
受付番号	5 9 9 0 0 8 3 2 0 3 5
書類名	特許願
担当官	坪 政光 8 8 4 4
作成日	平成 1 1 年 9 月 2 日

< 認定情報・付加情報 >

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
【氏名又は名称】	富士通株式会社

【特許出願人】

【識別番号】	000005108
【住所又は居所】	東京都千代田区神田駿河台四丁目 6 番地
【氏名又は名称】	株式会社日立製作所

【特許出願人】

【識別番号】	000004167
【住所又は居所】	東京都港区赤坂 4 丁目 1 4 番 1 4 号
【氏名又は名称】	日本コロムビア株式会社

【特許出願人】

【識別番号】	000001889
【住所又は居所】	大阪府守口市京阪本通 2 丁目 5 番 5 号
【氏名又は名称】	三洋電機株式会社

【代理人】

申請人	
【識別番号】	100064746
【住所又は居所】	大阪府大阪市北区南森町 2 丁目 1 番 2 9 号 住友 銀行南森町ビル 深見特許事務所
【氏名又は名称】	深見 久郎

【選任した代理人】

【識別番号】	100085132
【住所又は居所】	大阪府大阪市北区南森町 2 丁目 1 番 2 9 号 住友 銀行南森町ビル 深見特許事務所
【氏名又は名称】	森田 俊雄

【選任した代理人】

【識別番号】	100091409
--------	-----------

次頁有

認定・付加情報 (続 き)

【住所又は居所】 大阪府大阪市北区南森町 2 - 1 - 2 9 住友銀行
南森町ビル 深見特許事務所

【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781

【住所又は居所】 大阪府大阪市北区南森町 2 - 1 - 2 9 住友銀行
南森町ビル 深見特許事務所

【氏名又は名称】 堀井 豊

次頁無

特願平 1 1 - 2 4 1 7 4 7

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 2 2 3]

1. 変更年月日 1 9 9 6 年 3 月 2 6 日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名 富士通株式会社

特願平 1 1 - 2 4 1 7 4 7

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日 1 9 9 0 年 8 月 3 1 日
[変更理由] 新規登録
住 所 東京都千代田区神田駿河台 4 丁目 6 番地
氏 名 株式会社日立製作所
2. 変更年月日 2 0 0 4 年 9 月 8 日
[変更理由] 住所変更
住 所 東京都千代田区丸の内一丁目 6 番 6 号
氏 名 株式会社日立製作所

特願平 1 1 - 2 4 1 7 4 7

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 4 1 6 7]

1. 変更年月日 1 9 9 0 年 8 月 2 1 日
[変更理由] 新規登録
住 所 東京都港区赤坂 4 丁目 1 4 番 1 4 号
氏 名 日本コロムビア株式会社
2. 変更年月日 2 0 0 2 年 1 0 月 2 2 日
[変更理由] 名称変更
住 所 東京都港区赤坂 4 丁目 1 4 番 1 4 号
氏 名 コロムビアミュージックエンタテインメント株式会社
3. 変更年月日 2 0 0 5 年 8 月 3 0 日
[変更理由] 住所変更
住 所 東京都港区六本木一丁目 4 番 3 3 号 六本木 2 1 森ビル
氏 名 コロムビアミュージックエンタテインメント株式会社

特願平 1 1 - 2 4 1 7 4 7

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 1 8 8 9]

1. 変更年月日	1 9 9 3 年 1 0 月 2 0 日
[変更理由]	住所変更
住 所	大阪府守口市京阪本通 2 丁目 5 番 5 号
氏 名	三洋電機株式会社